# 48-Port GbE Web Smart Switch with 4 SFP Dual Media User's Manual

Release 1.30

# Table of Contents


Caution ..... vi

Electronic Emission Notices ..... vi

**1. Introduction ..... 1**

1-1. Overview of 48 Gigabit Web Smart Switch ..... 1

1-2. Checklist ..... 2

1-3. User Interfaces on the Front Panel (Button, LEDs and Plugs) ..... 3

1-4. User Interfaces on the Rear Panel ..... 4

**2. Installation ..... 5**

2-1. Starting 48 Gigabit Web Smart Switch Up ..... 5
2-1-1. Hardware and Cable Installation ..... 5
2-1-2. Installing Chassis to a 19-Inch Wiring Closet Rail ..... 7
2-1-3. Cabling Requirements ..... 7
2-1-4. Configuring the Management Agent of 48 Gigabit Web Smart Switch ..... 9

**3. Operation of Web-based Management ..... 10**

3-1. System ..... 11
3-1-1. System Information ..... 12
3-1-2. IP Configuration ..... 14
3-1-3. Time Configuration ..... 16
3-1-4. Account Configuration ..... 19

3-2. Port Configuration ..... 20
3-2-1. Port Status ..... 20
3-2-2. Port Configuration ..... 24
3-2-3. Simple Counter ..... 26
3-2-4. Detail Counter ..... 28

3-3. Storm ..... 32

3-4. Mirror ..... 34

3-5. Filter ..... 36

3-6. QoS ..... 38
3-6-1. Priority ..... 38
3-6-2. Policer Configuration ..... 44
3-6-3. Shaper Setting ..... 46
3-6-4. Flow ..... 48
3-6-5. Police-Flow ..... 52
3-6-6. Mark ..... 53
3-6-7. Mark-enable ..... 55

3-7. ACL ..... 56

3-8. ACL QoS Load ..... 63

3-9. User Defined ..... 64

3-10. SNMP Configuration ..... 65

3-11. Link Aggregation ..... 67
3-12. Alarm Configuration ..... 69
3-13. Configuration ..... 72
3-14. Diagnostics ..... 76
3-15. Loop Detection ..... 79
3-16. TFTP Server ..... 80
3-17. Log ..... 81
3-18. Firmware Upgrade ..... 83
3-19. Max. Packet Length ..... 84
3-21. VLAN ..... 88
3-21-1. VLAN Mode ..... 88
3-21-2. VLAN Group ..... 90
3-21-3. Port Protocol ..... 94
3-21-4. Port VID ..... 96
3-22. Reboot ..... 98
3-23. Logout ..... 99
**4. Operation of CLI Management ..... 100**
4-1. CLI Management ..... 100
4-1-1. Login ..... 100
4-2. Commands of CLI ..... 102
4-2-1. Global Commands of CLI ..... 103
4-2-2. Local Commands of CLI ..... 109
**5. FAQ ..... 114**
5-1. Resolving No Link Condition ..... 114
5-2. Q&A ..... 114
**Appendix A Technical Specifications ..... 115**

# Revision History

| Release | Date | Revision |
|---|---|---|
| 1.30 | 02/21/2008 | A1 |

## *Caution*

Circuit devices are sensitive to static electricity, which can damage their delicate electronics. Dry weather conditions or walking across a carpeted floor may cause you to acquire a static electrical charge.

To protect your device, always:

- Touch the metal chassis of your computer to ground the static electrical charge before you pick up the circuit device.
- Pick up the device by holding it on the left and right edges only.

## *Electronic Emission Notices*

### Federal Communications Commission (FCC) Statement

This equipment has been tested and found to comply with the limits for a class A computing device pursuant to Subpart J of part 15 of FCC Rules, which are designed to provide reasonable protection against such interference when operated in a commercial environment.

### European Community (CE) Electromagnetic Compatibility Directive

This equipment has been tested and found to comply with the protection requirements of European Emission Standard EN55022/EN60555-2 and the Generic European Immunity Standard EN50082-1.

| | | |
|---|---|---|
| EMC: | EN55022(1988)/CISPR-22(1985) | class A |
| | EN60555-2(1995) | class A |
| | EN60555-3 | |
| | IEC1000-4-2(1995) | 4K V CD, 8KV, AD |
| | IEC1000-4-3(1995) | 3V/m |
| | IEC1000-4-4(1995) | 1KV – (power line), 0.5KV – (signal line) |

# 1. Introduction

## 1-1. Overview of 48 Gigabit Web Smart Switch

48-port Gigabit Web Smart Switch is a standard switch that meets all IEEE 802.3/u/x/z Gigabit, Fast Ethernet specifications. The switch included 44 Port 10/100/1000Mbps TP and 4 Port Gigabit TP/SFP Fiber. The switch can be managed through Ethernet port using Web-based management unit, associated with web-based management, the network administrator can logon the switch to monitor, configure and control each port's activity. In addition, the switch implements the QoS (Quality of Service), VLAN, and Trunking. It is suitable for office application.

In this switch, Port 45 - 48 include two types of media --- TP and SFP Fiber (LC, BiDi-LC…); this port supports 10/100/1000Mbps TP or 1000Mbps SFP Fiber with auto-detected function. 1000Mbps SFP Fiber transceiver is used for high-speed connection expansion.

### Key Features in the Device

QoS-ACL:

The switch offers powerful QoS function. This function supports TOS field of IP header (equal DSCP low 3 bits) on Layer 3 of network framework and ACL.

VLAN:

Supports Port-based VLAN, IEEE802.1Q Tag VLAN. And supports 256 active VLANs and VLAN ID 1~4094.

Port Trunking:

Allows one or more links to be aggregated together to form a Link Aggregation Group by the static setting.

*Publication date: Feb., 2008*
*Revision A1*

## 1-2. Checklist

Before you start installing the switch, verify that the package contains the following:

- A set of Gigabit Web Smart Switch
- Mounting Accessory (for 19” Rack Shelf)
- This User's Manual in CD-ROM
- AC Power Cord

Please notify your sales representative immediately if any of the aforementioned items is missing or damaged.

*Publication date: Feb., 2008*
*Revision A1*

## 1-3. User Interfaces on the Front Panel (Button, LEDs and Plugs)

There are 48 TP Gigabit Ethernet ports and 4 SFP fiber ports for optional removable modules on the front panel of the switch. LED display area, locating on the left side of the panel, contains a Power LED, which indicates the power status and CPU working status of the switch.

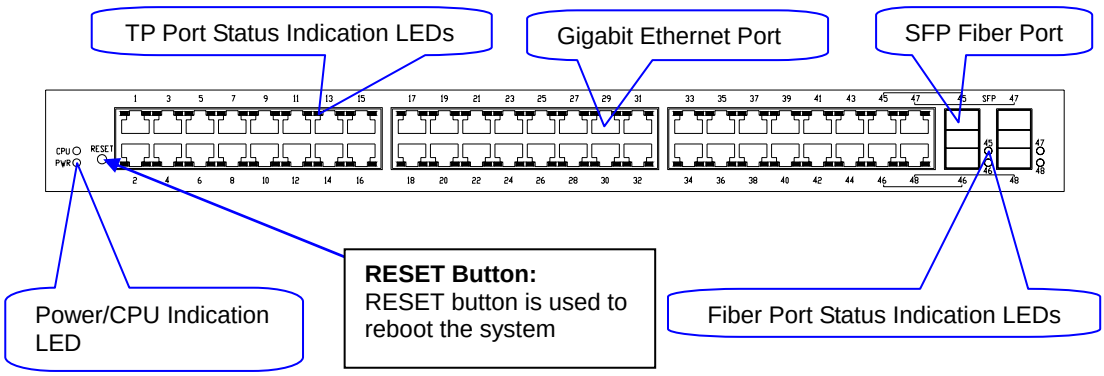



Fig. 1-1 Front View of 48 Gigabit Web Smart Switch

- **LED Indicators**

| LED | Color | Function |
|---|---|---|
| **System LED** | | |
| POWER | Green | Lit when +3.3V DC power is on and good |
| **10/100/1000Ethernet TP Port 1 to 48 LED** | | |
| LINK/ACT | Green | Lit when connection with remote device is good<br>Blinks when any traffic is present<br>Off when cable connection is not good |
| 10/100/1000Mbps | Green | Lit green when 1000Mbps speed is active<br>Blink green when 100Mbps speed is active<br>Off when 10Mbps speed is active |
| **1000SX/LX Gigabit Fiber Port 44 - 48 LED** | | |
| SFP(LINK/ACT) | Green | Lit when connection with the remote device is good<br>Blinks when any traffic is present<br>Off when module connection is not good |
| CPU | Green | Blinks when the switch works normally<br>Off when CPU fails or initializes |

Table1-1

## 1-4. User Interfaces on the Rear Panel

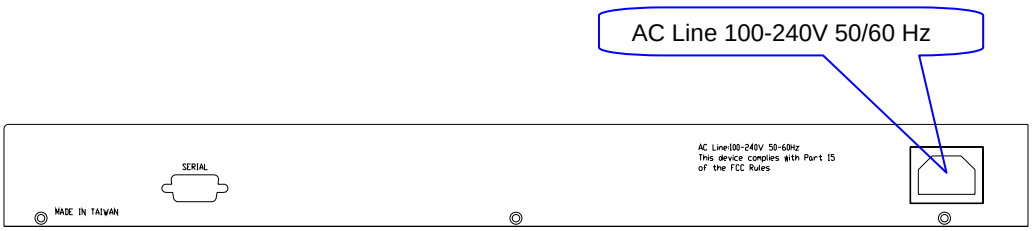



Fig. 1-2 Rear View of 48 Gigabit Web Smart Switch

# 2. Installation

## 2-1. Starting 48 Gigabit Web Smart Switch Up

This section will give users a quick start for:

- Hardware and Cable Installation
- Management Station Installation
- Software booting and configuration

### 2-1-1. Hardware and Cable Installation

At the beginning, please do first:

⇒ Wear a grounding device to avoid the damage from electrostatic discharge

- **Installing Optional SFP Fiber Transceivers to the 48 Gigabit Web Smart Switch**

  Note: If you have no modules, please skip this section.

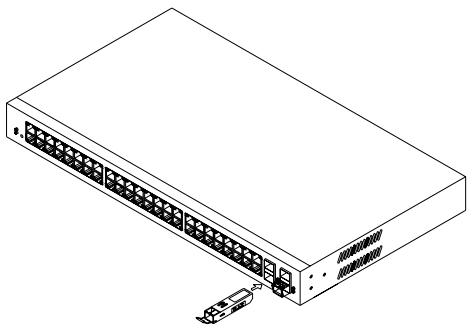


Fig. 2-1 Installation of Optional SFP Fiber Transceiver

- **Connecting the SFP Module to the Chassis:**

  The optional SFP modules are hot swappable, so you can plug or unplug it before or after powering on.

  1. Verify that the SFP module is the right model and conforms to the chassis
  2. Slide the module along the slot. Also be sure that the module is properly seated against the slot socket/connector
  3. Install the media cable for network connection
  4. Repeat the above steps, as needed, for each module to be installed into slot(s)

- **SFP Transceivers Supported**

This device is designed to support the SFP transceivers from the following manufactures:

- Black Box Corporation
- Avago Technologies (former Agilent Technologies)
- Finisa Corporation

SFP modules from other manufactures are not supported.

- **TP Port and Cable Installation**

⇒ In the switch, TP port supports MDI/MDI-X auto-crossover, so both types of cable, straight-through and crossed-over can be used. It means you do not have to tell from them, just plug it.

⇒ Use Cat. 5 grade RJ-45 TP cable to connect to a TP port of the switch and the other end is connected to a network-aware device.
⇒ Repeat the above steps, as needed, for each RJ-45 port to be connected to a Gigabit 10/100/1000 TP device.

Now, you can start having the switch in operation.

- **Power On**

The switch supports 100-240 VAC, 50-60 Hz power supply. The power supply will automatically convert the local AC power source to DC power. It does not matter whether any connection plugged into the switch or not when power on, even modules as well.

### 2-1-2. Installing Chassis to a 19-Inch Wiring Closet Rail

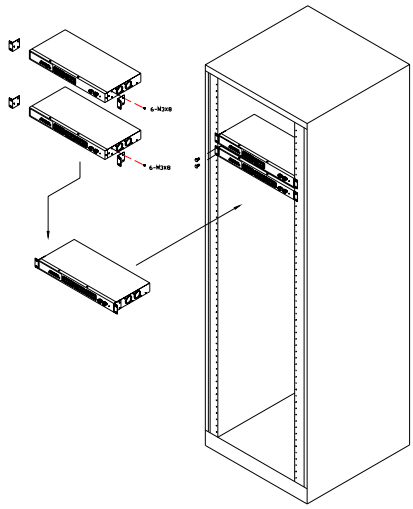


Fig. 2-2

**Caution: Allow a proper spacing and proper air ventilation for the cooling fan at both sides of the chassis.**

⇒ Wear a grounding device for electrostatic discharge.
⇒ Screw the mounting accessory to the front side of the switch (See Fig. 2-2).
⇒ Place the Chassis into the 19-inch wiring closet rail and locate it at the proper position. Then, fix the Chassis by screwing it.

### 2-1-3. Cabling Requirements

To help ensure a successful installation and keep the network performance good, please take a care on the cabling requirement. Cables with worse specification will render the LAN to work poorly.

### 2-1-3-1. Cabling Requirements for TP Ports

⇒ For Fast Ethernet TP network connection
  — The grade of the cable must be at least Cat. 5 with a maximum length of 100 meters.

⇒ Gigabit Ethernet TP network connection
  — The grade of the cable must be at least Cat. 5 with a maximum length of 100 meters. Cat. 5e is recommended.

## 2-1-4. Configuring the Management Agent of 48 Gigabit Web Smart Switch

Web-based UI for the switch is an interface in a highly friendly way. You can configure and monitor the switch through the switch's Ethernet port.

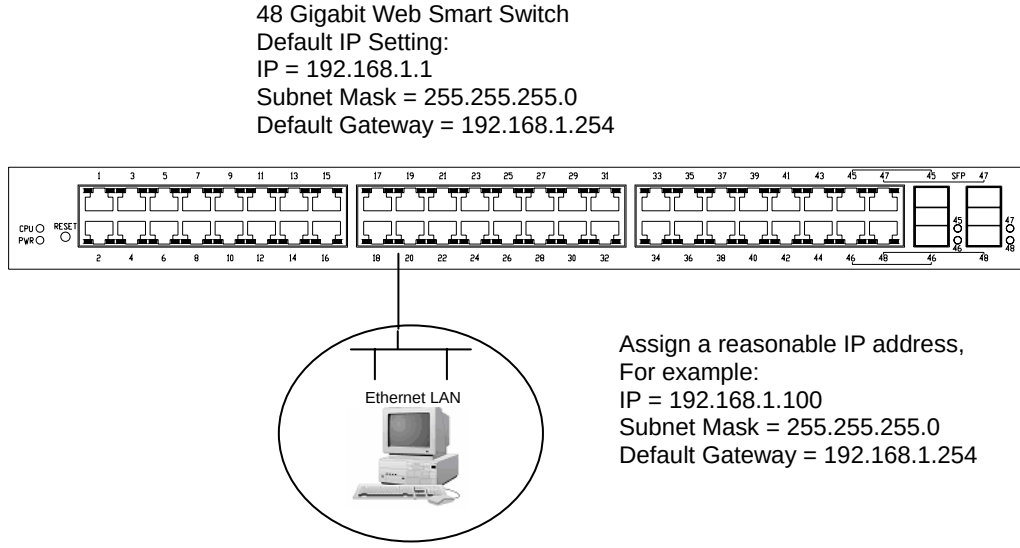



Fig. 2-3

- **Managing 48 Gigabit Web Smart Switch through Ethernet Port**

Before you communicate with the switch, you have to finish first the configuration of the IP address or to know the IP address of the switch. Then, follow the procedures listed below.

1. Set up a physical path between the configured the switch and a PC by a qualified cable with RJ-45 connector.

   Note: If PC directly connects to the switch, you have to setup the same subnet mask between them. But, subnet mask may be different for the PC in the remote site. Please refer to Fig. 2-3 about the Gigabit Web Smart Switch default IP address information.

2. Run web browser and follow the menu. Please refer to Chapter 3.

# 3. Operation of Web-based Management

This chapter instructs you how to configure and manage the 48 Gigabit Web Smart Switch through the web user interface it supports, to access and manage 44 10/100/1000Mbps TP Port and 4 Gigabit TP/SFP Fiber dual media port. The switch provides 44 fixed Gigabit Ethernet TP ports and 4 optional Gigabit dual media ports supporting either fiber or TP media. With this facility, you can easily access and monitor through any one port of the switch all the status of the switch, including each port activity, multicast traffic, and so on.

The default values of 48 Gigabit Web Smart Switch are listed in the table below:

| | |
|---|---|
| **IP Address** | 192.168.1.1 |
| **Subnet Mask** | 255.255.255.0 |
| **Default Gateway** | 192.168.1.254 |
| **Password** | admin |

Table 3-1

After the 48 Gigabit Web Smart Switch has been finished configuration, you can browse it by using the IP address you set up. For instance, type http://192.168.1.1 in the address row in a browser, it will show the following screen (see Fig.3-1) and ask you inputting password in order to login and access authentication. The default password is “admin”. For the first time to use, please enter the default password, then click the **<Apply>** button. The login process now is completed.

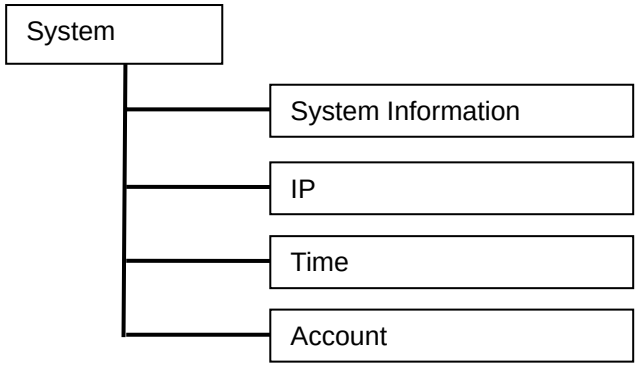
In the switch, it supports a simple user management function allowing only one administrator to configure the system at the same time.

To optimize the display effect, we recommend you use Microsoft IE 6.0 above, Netscape V7.1 above or FireFox V1.00 above and have the resolution 1024x768. The switch supported neutral web browser interface.

In Fig. 3-1, for example, left section is the whole function tree with web user interface and we will travel it through this chapter.

## 3-1. System

Four functions, including System Information, IP Configuration, Time and Account setting are contained in this function folder for system and network management. Each of them will be described in detail orderly in the following sections.



### 3-1-1. System Information

*Function name:*

System Information

*Function description:*

Show the basic system information.

*Parameter description:*

Model name:

The model name of this device.

System description:

It shows what this device is. Here, it is “Web Smart Managed Switch”.

Location:

Basically, it is the location where this switch is put for user-defining.

Contact:

In order to easily manage and maintain device, you may write down the contact person and phone here for getting help soon. You can configure this parameter through the device’s user interface or SNMP.

Device name:

The name of the switch that could be for user-defining.

System Up time:

The time accumulated since this switch is powered up. Its format is “day, hour, minute, second”.

Current time:

Show the system time of the switch. Its format is ”day of week, month, day, hours : minutes : seconds, year”. For instance, “Wed Apr 23 12:10:10 2004”.

BIOS version:

The version of the BIOS in this switch.

Firmware version:

The firmware version in this switch.

Hardware-Mechanical version:

The version of Hardware and Mechanical. The figure before the hyphen is the version of electronic hardware; the other after the hyphen is the version of mechanical.

Serial number:

The serial number is assigned by the manufacturer.

Host IP address:

The IP address of the switch.

Host MAC address:

It is the Ethernet MAC address of the management agent in this switch.

Device Port:

Show all types and numbers of the ports in the switch.

RAM size:

The size of the DRAM in this switch.

Flash size:

The size of the flash memory in this switch.

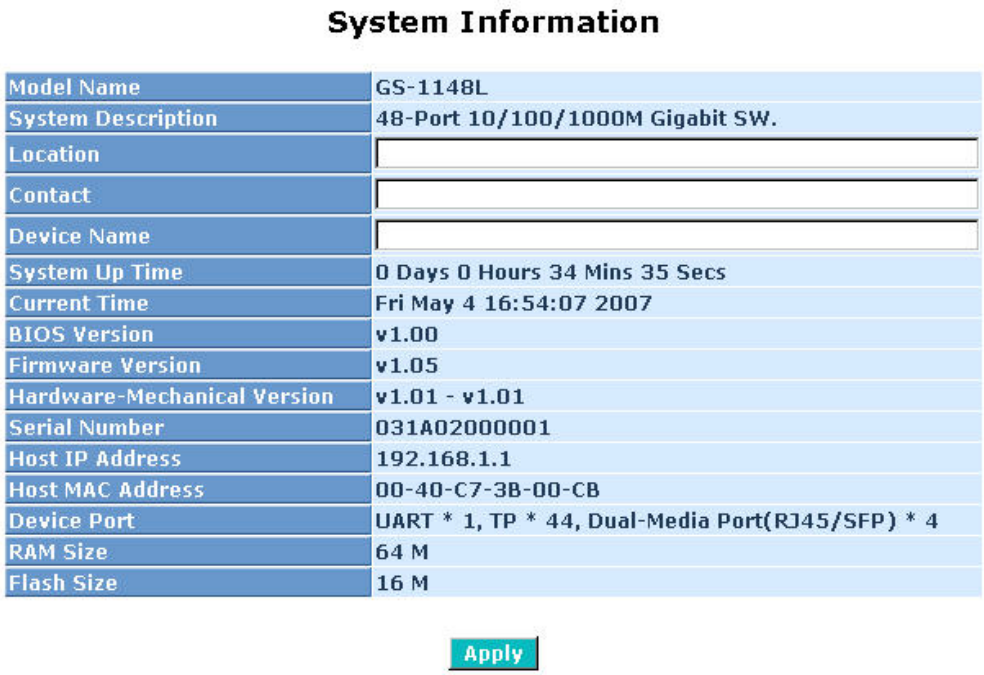



Fig. 3-1

### 3-1-2. IP Configuration

IP configuration is one of the most important configurations in the switch. Without the proper setting, network manager will not be able to manage or view the device. The switch supports both manual IP address setting. When IP address is changed, you must reboot the switch to have the setting taken effect and use the new IP to browse for web management and CLI management.

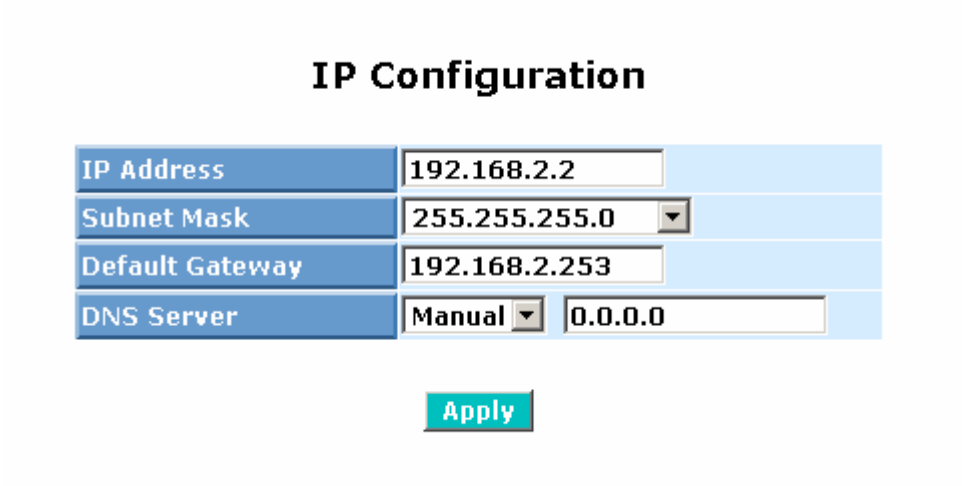



Fig. 3-2

*Function name:*

IP Configuration

*Function description:*

Set IP address, subnet mask, default gateway and DNS for the switch.

*Parameter description:*

IP address:

Users can configure the IP settings and fill in new values if users set the DHCP function “Disable”. Then, click **<Apply>** button to update the IP address.

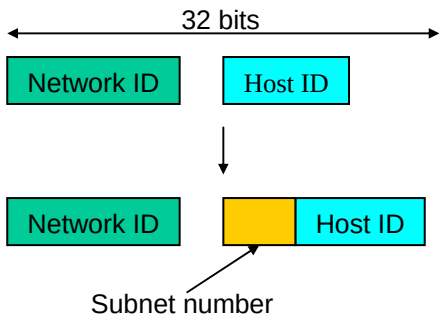
When DHCP is disabled, Default: 192.168.1.1

If DHCP is enabled, this field is filled by DHCP server and will not allow user manually set it any more.

Subnet mask:

Subnet mask is made for the purpose to get more network address because any IP device in a network must own its IP address, composed of Network address and Host address, otherwise can’t communicate with other devices each other.

But unfortunately, the network classes A, B, and C are all too large to fit for almost all networks, hence, subnet mask is introduced to solve this problem. Subnet mask uses some bits from host address and makes an IP address looked Network address, Subnet mask number and host address. It is shown in the following figure. This reduces the total IP number of a network able to support, by the amount of 2 power of the bit number of subnet number (2^(bit number of subnet number)).




Subnet mask is used to set the subnet mask value, which should be the same value as that of the other devices resided in the same network it attaches.

Default gateway:

Set an IP address for a gateway to handle those packets that do not meet the routing rules predefined in the device. If a packet does not meet the criteria for other pre-defined path, it must be forwarded to a default router on a default path. This means any packet with undefined IP address in the routing table will be sent to this device unconditionally.

Default: 192.168.1.254

DNS Server:

It is Domain Name Server used to serve the translation between IP address and name address.

The switch supports DNS client function to re-route the mnemonic name address to DNS server to get its associated IP address for accessing Internet. User can specify a DNS IP address for the switch. With this, the switch can translate a mnemonic name address into an IP address.

There are two ways to specify the IP address of DNS. One is fixed mode, which manually specifies its IP address, the other is dynamic mode, which is assigned by DHCP server while DHCP is enabled. DNS can help you easily remember the mnemonic address name with the meaningful words in it. Default is no assignment of DNS address.

Default: 0.0.0.0

### 3-1-3. Time Configuration

The switch provides manual and automatic ways to set the system time via NTP. Manual setting is simple and you just input “Year”, “Month”, “Day”, “Hour”, “Minute” and “Second” within the valid value range indicated in each item. If you input an invalid value, for example, 61 in minute, the switch will clamp the figure to 59.

NTP is a well-known protocol used to synchronize the clock of the switch system time over a network. NTP, an internet draft standard formalized in RFC 1305, has been adopted on the system is version 3 protocol. The switch provides four built-in NTP server IP addresses resided in the Internet and an user-defined NTP server IP address. The time zone is Greenwich-centered which uses the expression form of GMT+/- xx hours.

*Function name:*

Time

*Function description:*

Set the system time by manual input or set it by syncing from Time servers. The function also supports daylight saving for different area’s time adjustment.

*Parameter description:*

Current Time:

Show the current time of the system.

Manual:

This is the function to adjust the time manually. Filling the valid figures in the fields of Year, Month, Day, Hour, Minute and Second respectively and press **<Apply>** button, time is adjusted. The valid figures for the parameter Year, Month, Day, Hour, Minute and Second are >=2000, 1-12, 1-31, 0-23, 0-59 and 0-59 respectively. Input the wrong figure and press **<Apply>** button, the device will reject the time adjustment request. There is no time zone setting in Manual mode.

Default: Year = 2000, Month = 1, Day = 1
Hour = 0, Minute = 0, Second = 0

NTP:

NTP is Network Time Protocol and is used to sync the network time based Greenwich Mean Time (GMT). If use the NTP mode and select a built-in NTP time server or manually specify an user-defined NTP server as well as Time Zone, the switch will sync the time in a short after pressing **<Apply>** button. Though it synchronizes the time automatically, NTP does not update the time periodically without user’s processing.

Time Zone is an offset time off GMT. You have to select the time zone first and then perform time sync via NTP because the switch will combine this time zone offset and updated NTP time to come out the local time, otherwise, you will not able to get the correct time. The switch supports configurable time zone from –12 to +13 step 1 hour.

Default Time zone: +8 Hrs.

Daylight Saving:

Daylight saving is adopted in some countries. If set, it will adjust the time lag or in advance in unit of hours, according to the starting date and the ending date. For example, if you set the day light saving to be 1 hour. When the time passes over the starting time, the system time will be increased one hour after one minute at the time since it passed over. And when the time passes over the ending time, the system time will be decreased one hour after one minute at the time since it passed over.

The switch supports valid configurable day light saving time is –5 ~ +5 step one hour. The zero for this parameter means it need not have to adjust current time, equivalent to in-act daylight saving. You don't have to set the starting/ending date as well. If you set daylight saving to be non-zero, you have to set the starting/ending date as well; otherwise, the daylight saving function will not be activated.

Default for Daylight Saving: 0.

The following parameters are configurable for the function Daylight Saving and described in detail.

Day Light Saving Start:

This is used to set when to start performing the day light saving time.

Mth:

Range is 1 ~ 12.

Default: 1

Day:

Range is 1 ~ 31.

Default: 1

Hour:

Range is 0 ~ 23.

Default: 0

Day Light Saving End:

This is used to set when to stop performing the daylight saving time.

Mth:

Range is 1 ~ 12.

Default: 1

Day:

Range is 1 ~ 31.

Default: 1

Hour:

Range is 0 ~ 23.

Default: 0

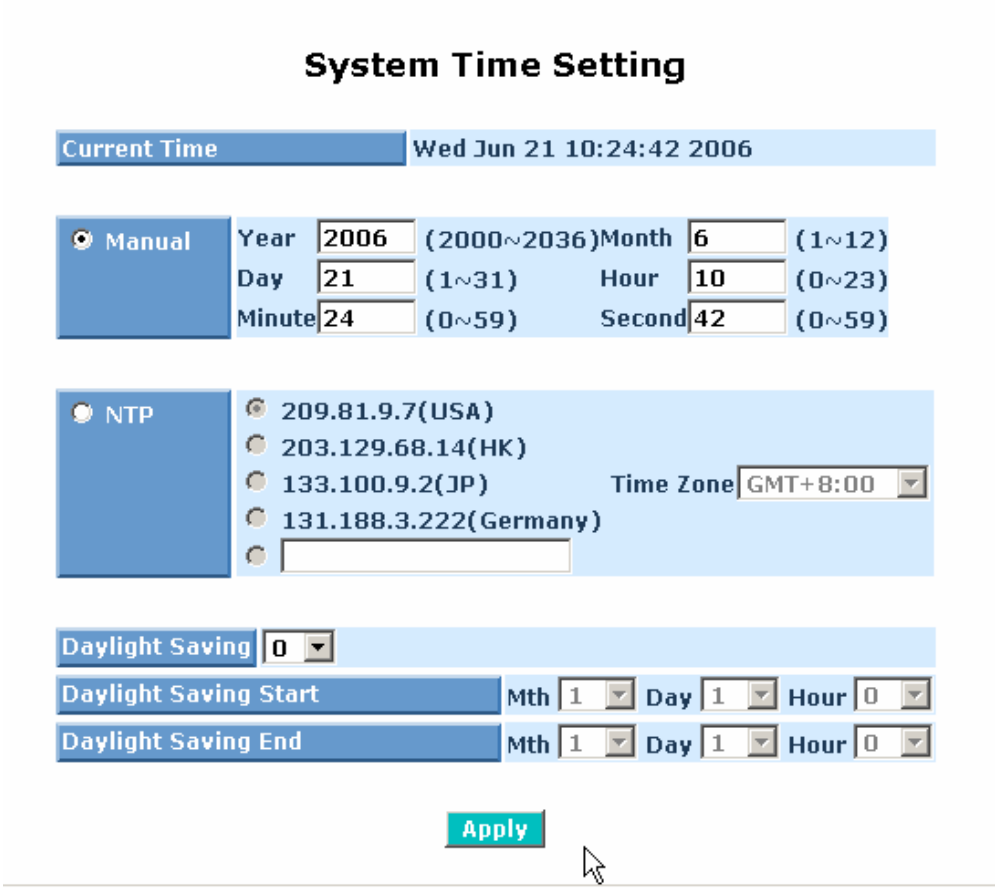



Fig. 3-3

### 3-1-4. Account Configuration

In this function, only administrator can create, modify or delete the username and password. Administrator can modify other guest identities' password without confirming the password but it is necessary to modify the administrator-equivalent identity. Guest-equivalent identity can modify his password only. Please note that you must confirm administrator/guest identity in the field of Authorization in advance before configuring the username and password. Only one administrator is allowed to exist and unable to be deleted. In addition, up to 4 guest accounts can be created.

The default setting for user account is:

Username : admin

Password : admin

The default setting for guest user account is:

Username : guest

Password : guest

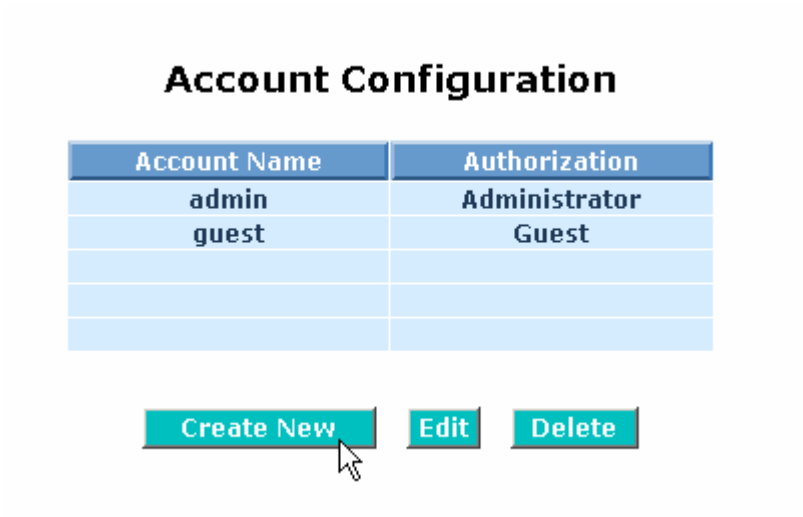
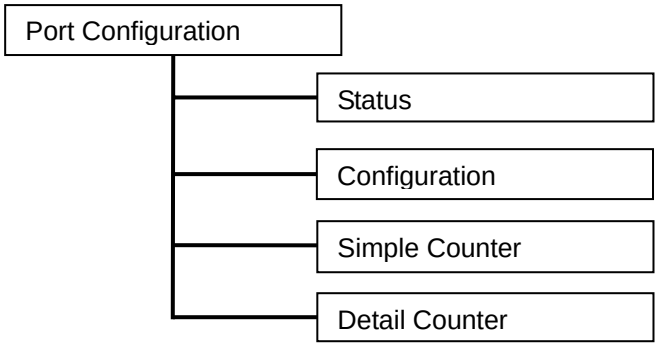



Fig. 3-4

## 3-2. Port Configuration

Four functions, including Port Status, Port Configuration, Simple Counter and Detail Counter are contained in this function folder for port monitor and management. Each of them will be described in detail orderly in the following sections.




### 3-2-1. Port Status

The function Port Status gathers the information of all ports' current status and reports it by the order of port number, link status, port state, Auto-Negotiation status, and speed/duplex and flow control. An extra media type information for the module ports 45, 46, 47, and 48 is also offered.

**Port Current Status**

| Port | Port Name | Media | Link | State | Auto Nego. | Speed/Duplex | Flow Control | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | | Transmit | Receive |
| 1 | | TP | Up | Enabled | Enabled | 100M/Full | Disabled | Disabled |
| 2 | | TP | Down | Enabled | Enabled | 1G/Half | Enabled | Enabled |
| 3 | | TP | Down | Enabled | Enabled | 1G/Half | Enabled | Enabled |
| 4 | | TP | Down | Enabled | Enabled | 1G/Half | Enabled | Enabled |
| 5 | | TP | Down | Enabled | Enabled | 1G/Half | Enabled | Enabled |
| 6 | | TP | Down | Enabled | Enabled | 1G/Half | Enabled | Enabled |
| 7 | | TP | Down | Enabled | Enabled | 1G/Half | Enabled | Enabled |
| 8 | | TP | Down | Enabled | Enabled | 1G/Half | Enabled | Enabled |
| 9 | | TP | Down | Enabled | Enabled | 1G/Half | Enabled | Enabled |
| 10 | | TP | Down | Enabled | Enabled | 1G/Half | Enabled | Enabled |
| 11 | | TP | Down | Enabled | Enabled | 1G/Half | Enabled | Enabled |
| 12 | | TP | Down | Enabled | Enabled | 1G/Half | Enabled | Enabled |
| 13 | | TP | Down | Enabled | Enabled | 1G/Half | Enabled | Enabled |
| 14 | | TP | Down | Enabled | Enabled | 1G/Half | Enabled | Enabled |
| 15 | | TP | Down | Enabled | Enabled | 1G/Half | Enabled | Enabled |
| 16 | | TP | Down | Enabled | Enabled | 1G/Half | Enabled | Enabled |
| 17 | | TP | Down | Enabled | Enabled | 1G/Half | Enabled | Enabled |
| 18 | | TP | Down | Enabled | Enabled | 1G/Half | Enabled | Enabled |
| 19 | | TP | Down | Enabled | Enabled | 1G/Half | Enabled | Enabled |
| 20 | | TP | Down | Enabled | Enabled | 1G/Half | Enabled | Enabled |
| 21 | | TP | Down | Enabled | Enabled | 1G/Half | Enabled | Enabled |
| 22 | | TP | Down | Enabled | Enabled | 1G/Half | Enabled | Enabled |

Fig. 3-5

Function name:

*Port Status*

Function Description:

Report the latest updated status of all ports in this switch. When any one of the ports in the switch changes its parameter displayed in the page, it will be automatically refreshed the port current status about every 5 seconds.

Parameter Description:

Port No:

Display the port number. The number is 1 – 48. Both port 45, 46,47and 48 are optional modules.

Media:

Show the media type adopted in all ports. The Port 45-48 are optional modules, which support either fiber or UTP media with either Gigabit Ethernet (1000Mbps) or 10/100Mbps Fast Ethernet port. They may have different media types and speed. Especially, fiber port has comprehensive types of connector, distance, fiber mode and so on.

Link:

Show that if the link on the port is active or not. If the link is connected to a working-well device, the Link will show the link “Up”; otherwise, it will show “Down”. This is determined by the hardware on both devices of the connection.

No default value.

State:

Show that the communication function of the port is “Enabled” or “Disabled”. When it is enabled, traffic can be transmitted and received via this port. When it is disabled, no traffic can be transferred through this port. Port State is configured by user.

Default: Enabled.

Auto Nego.:

Show the exchange mode of Ethernet MAC. There are two modes supported in the switch. They are auto-negotiation mode “Enabled” and forced mode “Disabled”. When in “Enabled” mode, this function will automatically negotiate by hardware itself and exchange each other the capability of speed and duplex mode with other site which is linked, and

comes out the best communication way. When in “Disabled” mode, both parties must have the same setting of speed and duplex, otherwise, both of them will not be linked. In this case, the link result is “Down”.

Default: Enabled

Speed / Duplex:

Display the speed and duplex of all port. There are three speeds 10Mbps, 100Mbps and 1000Mbps supported for TP media, and the duplex supported is half duplex and full duplex. If the media is 1Gbps fiber, it is 1000Mbps supported only. The status of speed/duplex mode is determined by 1) the negotiation of both local port and link partner in "Auto Speed" mode or 2) user setting in "Force" mode. The local port has to be preset its capability.

Default: None, depends on the result of the negotiation.

Flow Control:

Show each port's flow control status of Transmit and Receive. You could control them in Port Configuration. When flow control status of Transmit is disabled in some port, the port will not transmit Pause Frame. However, When flow control status of Receive is disabled in some port, the port will have no effect and not handle the Pause Frame if it receives Pause Frame.

Default of Transmit and Receive: Enable

### 3-2-2. Port Configuration

Port Configuration is applied to change the setting of each port, including Port Name, Status, Speed Mode, and Flow Control Status. All of them are described in detail below. You can click the hyper-link of Port No. to configure Port Configuration. As you disable Port Status, the port will not transmit, receive and deal with packets. Flow Control will prevent the congestion from happening in real-network situation.

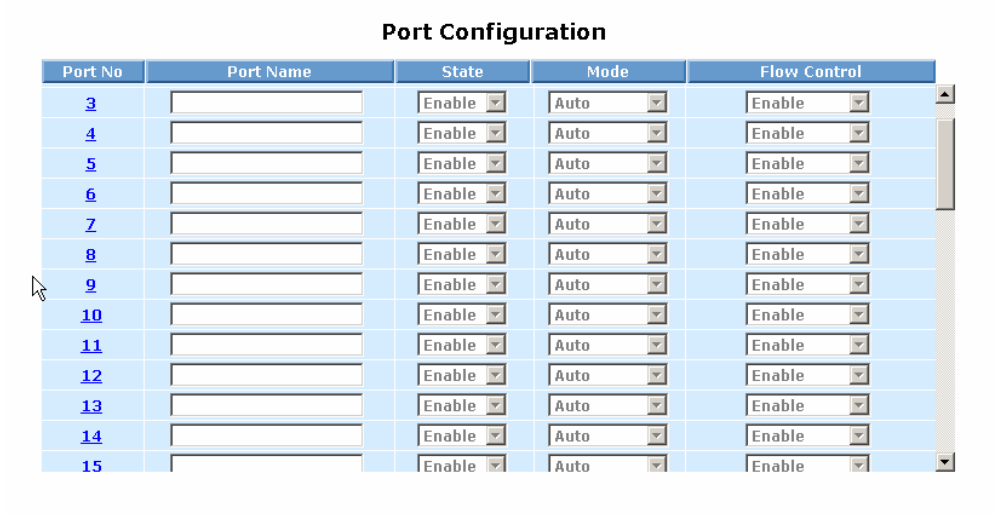



Fig. 3-6

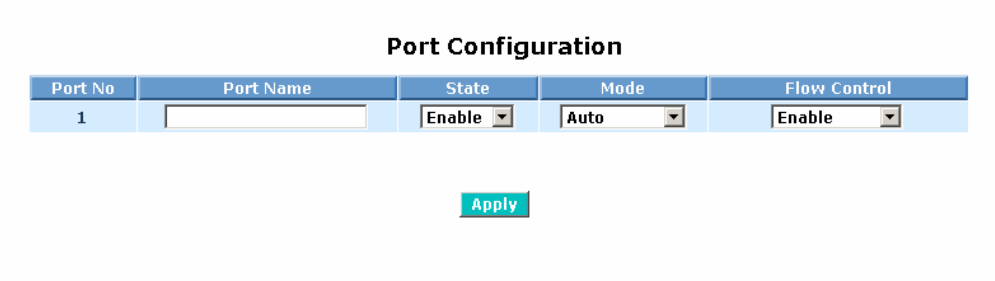



Fig. 3-7

*Function name:*

Port Configuration

*Function description:*

It is used to set each port's operation mode. You can fill special Port Name for each port. You also change the setting of Port Status, Port Transmitting Mode and Flow Control Status.

*Parameter description:*

Port Name:

Assign the special name of each port. You can fill any characters such as alphabets in the port name field.

State:

Set the communication capability of the port is Enabled or Disabled. When enabled, traffic can be transmitted and received via this port. When disabled, the port is blocked and no traffic can be transferred through this port. Port State is configurable by the user. There are only two states "Enable" and "Disable" able to choose. If you set a port's state "Disable", then that port is prohibited to pass any traffic, even it looks Link up.

Default: Enable.

Mode:

Set the speed and duplex of the port. In speed, if the media is 1Gbps fiber, it is always 1000Mbps and the duplex is full only. If the media is TP, the Speed/Duplex is comprised of the combination of speed mode, 10/100/1000Mbps, and duplex mode, full duplex and half duplex. The following table summarized the function the media supports.

| Media type | NWay | Speed | Duplex |
|---|---|---|---|
| 1000M TP | ON/OFF | 10/100/1000M | Full for all, Half for 10/100 |
| 1000M Fiber | ON/OFF | 1000M | Full |

In Auto-negotiation mode, no default value. In Forced mode, default value depends on your setting.

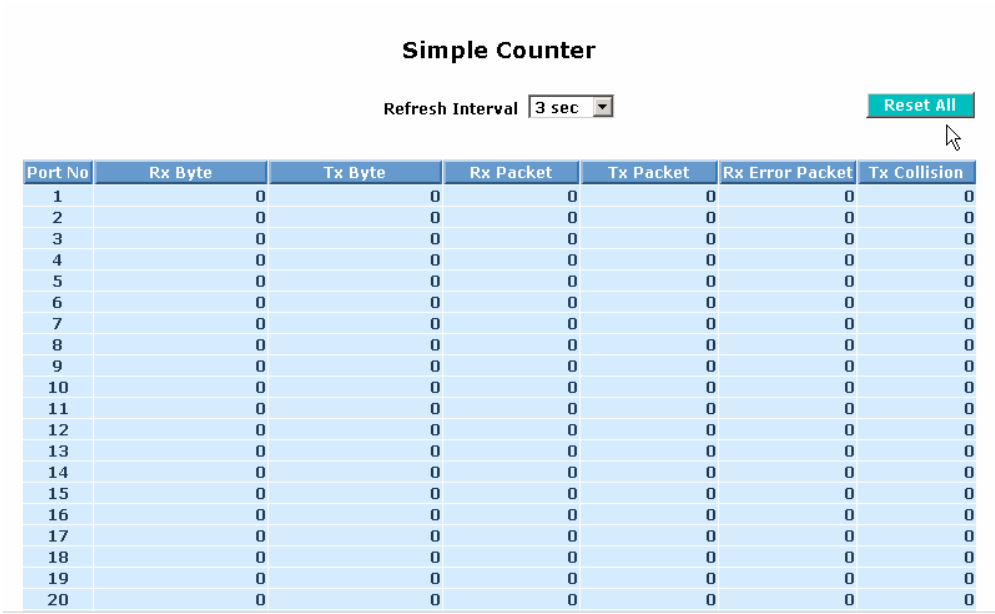
Flow Control:

There are two modes to choose in flow control, including Enable and Disable on the manners of Transmit and Receive. If flow control is set as Enable on some port, the port can send PAUSE frame to the transmitting device(s) as the receiving port is too busy to handle. Moreover, the port will decrease the transmitting speed as it captures the pause frames transmitted from others ports. When it is set as Disable, there will be no flow control capability in the port. It drops the packet if too much to handle. If flow control is set as Enable of Receive of some port, the port will decrease the transmitting speed as it gets the pause frames. This feature is "Enable" by Default.

### 3-2-3. Simple Counter

The function of Simple Counter collects any information and provides the counting about the traffic of the port, no matter the packet is good or bad.

In the Fig. 3-8, the window can show all ports' counter information at the same time. Each data field has 20-digit long. If the counting is overflow, the counter will be reset and restart counting. The data is updated every time interval defined by the user. The valid range is 3 to 10 seconds. The Refresh Interval is used to set the update frequency. Default update time is 3 seconds.




| Port No | Rx Byte | Tx Byte | Rx Packet | Tx Packet | Rx Error Packet | Tx Collision |
|---|---|---|---|---|---|---|
| 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| 2 | 0 | 0 | 0 | 0 | 0 | 0 |
| 3 | 0 | 0 | 0 | 0 | 0 | 0 |
| 4 | 0 | 0 | 0 | 0 | 0 | 0 |
| 5 | 0 | 0 | 0 | 0 | 0 | 0 |
| 6 | 0 | 0 | 0 | 0 | 0 | 0 |
| 7 | 0 | 0 | 0 | 0 | 0 | 0 |
| 8 | 0 | 0 | 0 | 0 | 0 | 0 |
| 9 | 0 | 0 | 0 | 0 | 0 | 0 |
| 10 | 0 | 0 | 0 | 0 | 0 | 0 |
| 11 | 0 | 0 | 0 | 0 | 0 | 0 |
| 12 | 0 | 0 | 0 | 0 | 0 | 0 |
| 13 | 0 | 0 | 0 | 0 | 0 | 0 |
| 14 | 0 | 0 | 0 | 0 | 0 | 0 |
| 15 | 0 | 0 | 0 | 0 | 0 | 0 |
| 16 | 0 | 0 | 0 | 0 | 0 | 0 |
| 17 | 0 | 0 | 0 | 0 | 0 | 0 |
| 18 | 0 | 0 | 0 | 0 | 0 | 0 |
| 19 | 0 | 0 | 0 | 0 | 0 | 0 |
| 20 | 0 | 0 | 0 | 0 | 0 | 0 |

Fig. 3-8

*Function name:*

Simple Counter

*Function description:*

Display the summary counting of each port's traffic, including Tx Byte, Rx Byte, Tx Packet, Rx Packet, Tx Collision and Rx Error Packet.

*Parameters description:*

Rx Byte:

Total received bytes.

Tx Byte:

Total transmitted bytes.

Rx Packet:

The counting number of the packet received.

Tx Packet:

The counting number of the packet transmitted.

Rx Error Packet:

Number of bad packets received.

Tx Collision:

Number of collisions transmitting frames experienced.

### 3-2-4. Detail Counter

The function of Detail Counter collects any information and provides the counting about the traffic of the port, no matter the packet is good or bad.

In the Fig. 3-9, the window can show only one port counter information at the same time. To see another port's counter, you have to pull down the list of Select, then you will see the figures displayed about the port you had chosen.

Each data field has 20-digit long. If the counting is overflow, the counter will be reset and restart counting. The data is updated every time interval defined by the user. The valid range is 3 to 10 seconds. The Refresh Interval is used to set the update frequency. Default update time is 3 seconds.

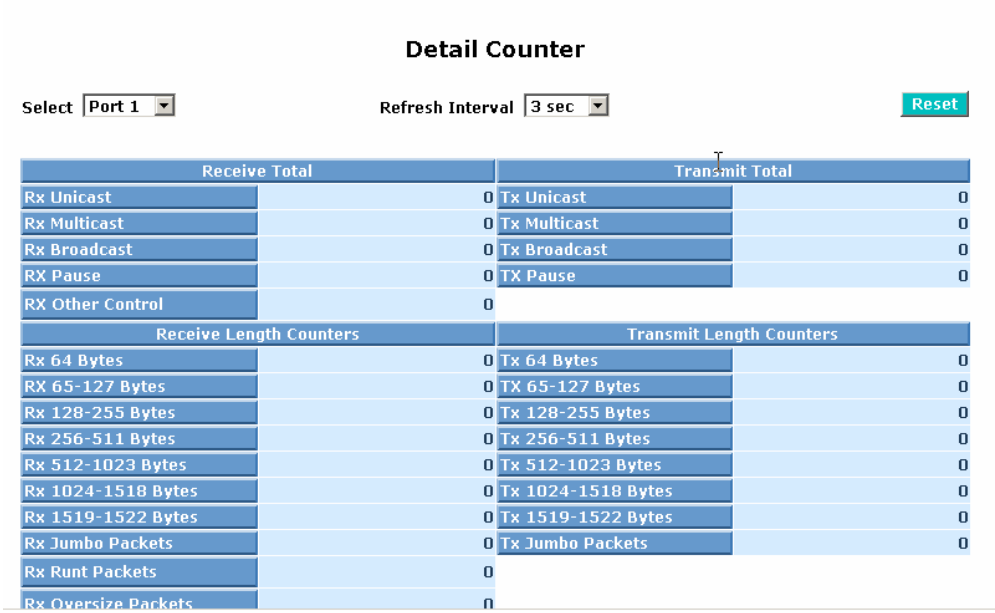



Fig. 3-9

*Function name:*

Detail Counter

*Function description:*

Display the detailed counting number of each port's traffic. In the Fig. 3-9, the window can show all counter information of each port at one time.

*Parameter description:*

Rx Unicast:

Show the counting number of the received unicast packet.

Rx Broadcast:

Show the counting number of the received broadcast packet.

Rx Multicast:

Show the counting number of the received multicast packet.

Rx Pause:

Show the counting number of the received Pause Frames.

Rx Other Control

Show the counting number of the received other packets.

Tx Unicast:

Show the counting number of the transmitted unicast packet.

Tx Broadcast:

Show the counting number of the transmitted broadcast packet.

Tx Multicast:

Show the counting number of the transmitted multicast packet.

Tx Pause:

Show the counting number of the transmitted Pause Frames.

Rx 64 Bytes:

Number of 64-byte frames in good and bad packets received.

Rx 65-127 Bytes:

Number of 65 ~ 126-byte frames in good and bad packets received.

Rx 128-255 Bytes:

Number of 127 ~ 255-byte frames in good and bad packets received.

Rx 256-511 Bytes:

Number of 256 ~ 511-byte frames in good and bad packets received.

Rx 512-1023 Bytes:

Number of 512 ~ 1023-byte frames in good and bad packets received.

Rx 1024-1518 Bytes:

Number of 1024-1518-byte frames in good and bad packets received.

Rx 1519-1522 Bytes:

Number of 1519-1522-byte frames in good and bad packets received.

Rx Jumbo Packets:

Number of packets which are up to 6 times the size of standard Ethernet packets. This field will show Number of Jumbo frames received.

Rx Runt Packets:

Collisions can generate runt packets that are less than 512 bits in length. This field will show the number of Runt Packets

Rx Oversize:

Number of long frames(according to max_length register) with valid CRC.

Tx 64 Bytes:

Number of 64-byte frames in good and bad packets transmitted.

Tx 65-127 Bytes:

Number of 65 ~ 126-byte frames in good and bad packets transmitted.

Tx 128-255 Bytes:

Number of 127 ~ 255-byte frames in good and bad packets transmitted.

Tx 256-511 Bytes:

Number of 256 ~ 511-byte frames in good and bad packets transmitted.

Tx 512-1023 Bytes:

Number of 512 ~ 1023-byte frames in good and bad packets transmitted.

Tx 1024-1518 Bytes:

Number of 1024-1518-byte frames in good and bad packets transmitted.

Tx 1519-1522 Bytes:

Number of 1519-1522-byte frames in good and bad packets transmitted.

Tx Jumbo Packets:

Number of packets which are up to 6 times the size of standard Ethernet packets. This field will show Number of Jumbo frames transmitted.

Rx CRC:

Number of Alignment errors and CRC error packets received.

Rx Code:

The number of packets received with a CRC error and a code error. These packets do not have dribble bits and are at least 64 bytes in length.

Rx Fragment:

Number of short frames (< 64 bytes) with invalid CRC.

Tx Single Collisions:

The number of packets successfully transmitted after experiencing one collisions.

Tx Multiple Collisions:

The number of packets successfully transmitted after experiencing multiple collisions.

Tx Excessive Collisions:

The number of packets successfully transmitted after experiencing excessive collisions.

Tx Late Collisions:

The number of packets that fail to be transmitted due to a late collision. Such packets may have experienced one or more normal collisions prior to the late collision.

Tx Deferred:

A count of all packets that had to defer to either traffic on the network (half-duplex mode) or to an active pause timer (full-duplex mode).

## 3-3. Storm

*Function name:*

Storm Control

*Function description:*

Storm Control is used to block unnecessary frames of the multicast and broadcast reducing the switch's performance. When the frames of the multicast or broadcast are over the rate and Strom Control enables, they could be determined to drop the frames of exceeded rate.

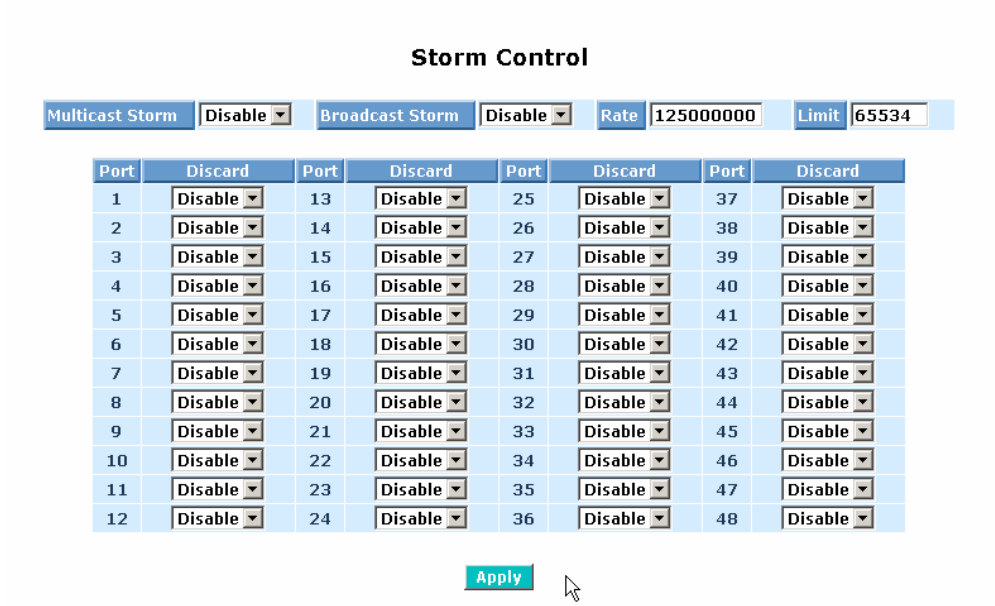



Fig. 3-10

*Parameter description:*

Multicast Storm:

To enable the Multicast Storm capability. Default is Disable.

Broadcast Storm:

To enable the Broadcast Storm capability. Default is Disable.

Rate:

The transmitting rate of Multicast or Broadcast packets. Default is 125000000 bytes. The setting range is 119~125000000.

Limit:

Limit is the buffer size of the switch and the maximum tolerated packets

of switch's buffer as well. This feature is "65534" by default.

Port:

There are 1~48 ports for your controlling Strom Control.

Discard:

To discard the frames of the multicast or broadcast exceeding the rate of Storm Control's configuration. Default is disable; you could enable storm control function for each port. After completing the function's setting, press **<Apply>** button to have this function taken effect.

## 3-4. Mirror

*Function name:*

Mirror

*Function description:*

Mirror Configuration is to monitor the traffic of the network. For example, we assume that Port A and Port B are Monitoring Port and Monitored Port respectively, thus, the traffic received by Port B will be copied to Port A for monitoring. First, you could decide to monitor the traffic of Ingress or Egress ports. And then, you should be determined to which ports you would like monitor.

*Parameter description:*

Mode:

Decide the modes of mirror, being disable, Ingress and Egress. When you choose Ingress, the traffic of Ingress of the monitored ports will be monitored. On the contrary, when you choose Egress, the traffic of Egress of the monitored ports will be monitored.

Monitoring Port:

To decide one as Monitoring port. Valid port is Port 1~48 and default is None.

Monitored Ports:

To configure the ports for being monitored. There are 1~48 ports. Just tick the check box (☑) beside the port x and press **<Apply>** button to have this function taken effect.

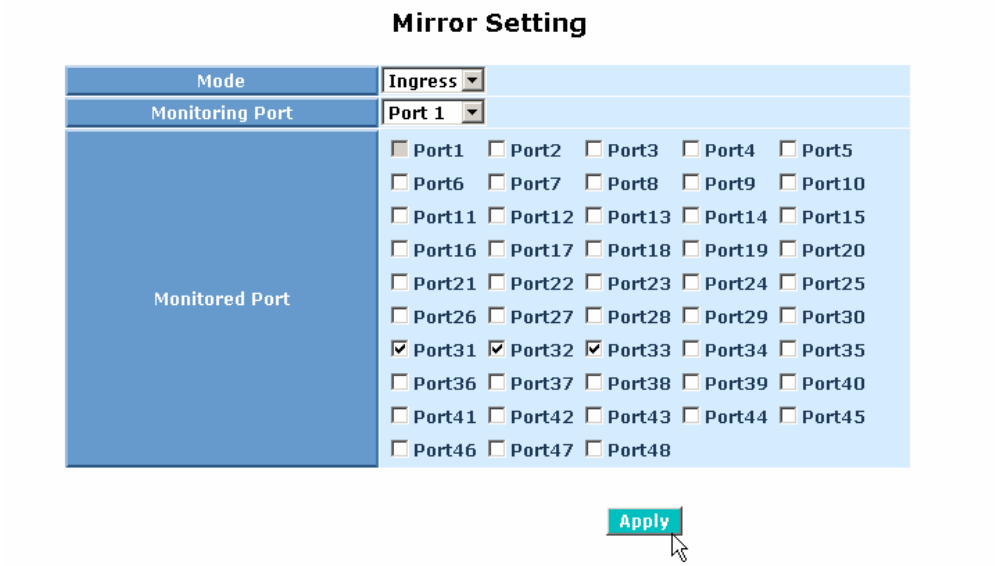

Mirror Setting
Mode
Ingress
Monitoring Port
Port 1
Monitored Port
Port1 Port2 Port3 Port4 Port5
Port6 Port7 Port8 Port9 Port10
Port11 Port12 Port13 Port14 Port15
Port16 Port17 Port18 Port19 Port20
Port21 Port22 Port23 Port24 Port25
Port26 Port27 Port28 Port29 Port30
Port31 Port32 Port33 Port34 Port35
Port36 Port37 Port38 Port39 Port40
Port41 Port42 Port43 Port44 Port45
Port46 Port47 Port48
Apply

Fig. 3-11

## 3-5. Filter

*Function name:*

Filter Setting

*Function description:*

Filter Setting can prevent the switch from some bad or unknown traffic and make the switch's performance better. It can filter the network traffic being Bad Length packet, Unknown Encapsulation packet, Unknown Ethertype frame, Unknown IP Protocol packet, IPv4 options packet, or Unknown Source Address packet. The switch will all accept completed and normal packets and block abnormal traffic flows.

*Parameter description:*

Filter Mode:

There are five options being Bad Length, Unknown Encapsulation, Unknown Ethertype, Unknown IP Protocol, IPv4 options, and Unknown Source Address packet for your using. Bad Length is a received packet's length field does not match the length of the packet's data field. Unknown Encapsulation is a received packet's encapsulation that is not Ethernet V2 or SNAP (with or without VLAN tag). Unknown Ethertype is a received packet's field that is not IPv4, IPv6, ARP, or RARP. Unknown IP Protocol is a received packet's IP protocol field that is not ICMP, IGMP, TCP and UDP. IPv4 options are that an IPv4 packet contains options.

Ports:

1~48 ports are for your selecting. Below ticking options (L.) are used to filter the traffic of the logical ports created by Link Aggregation. Tick "All" option will click all physical ports rapidly. After completing the function's setting, press **<Apply>** button to have this function taken effect.

Bad Length Filtering
Port 1
Port 2
Port 3
Port 4
Port 5
Port 6
Port 7
Port 8
Port 9
Port 10
Port 11
Port 12
Port 13
Port 14
Port 15
Port 16
Port 17
Port 18
Port 19
Port 20
Port 21
Port 22
Port 23
Port 24
Port 25
Port 26
Port 27
Port 28
Port 29
Port 30
Port 31
Port 32
Port 33
Port 34
Port 35
Port 36
Port 37
Port 38
Port 39
Port 40
Port 41
Port 42
Port 43
Port 44
Port 45
Port 46
Port 47
Port 48
All
Apply

Fig. 3-12

## 3-6. QoS
### 3-6-1. Priority

*Function name:*

Priority Configuration

*Function description:*

There are five settings of Priority Configuration for your using. Those are IP Layer Priority State Setting, Differentiated Service Code Point(DSCP), Port Priority Setting, Queue, and ACL-override. In the switch, there are three modes of QoS will take effect. There are DSCP, 802.1p and Port Priority respectively. The precedence of them are DSCP > 802.1p > Port Priority so when you want to use QoS of 802.1p or Port Priority of some ports, these ports should enable IP-ignored in advance. Furthermore, the scheduling of QoS uses Strict Priority. The higher priority of packet will get the highest precedence to transit in the switch. In Priority Configuration, if you would like the priority of ACL override the other priorities of QoS, such as DSCP, you could enable ACL-enabled in some ports. 802.1p is the priority of vlan tag.

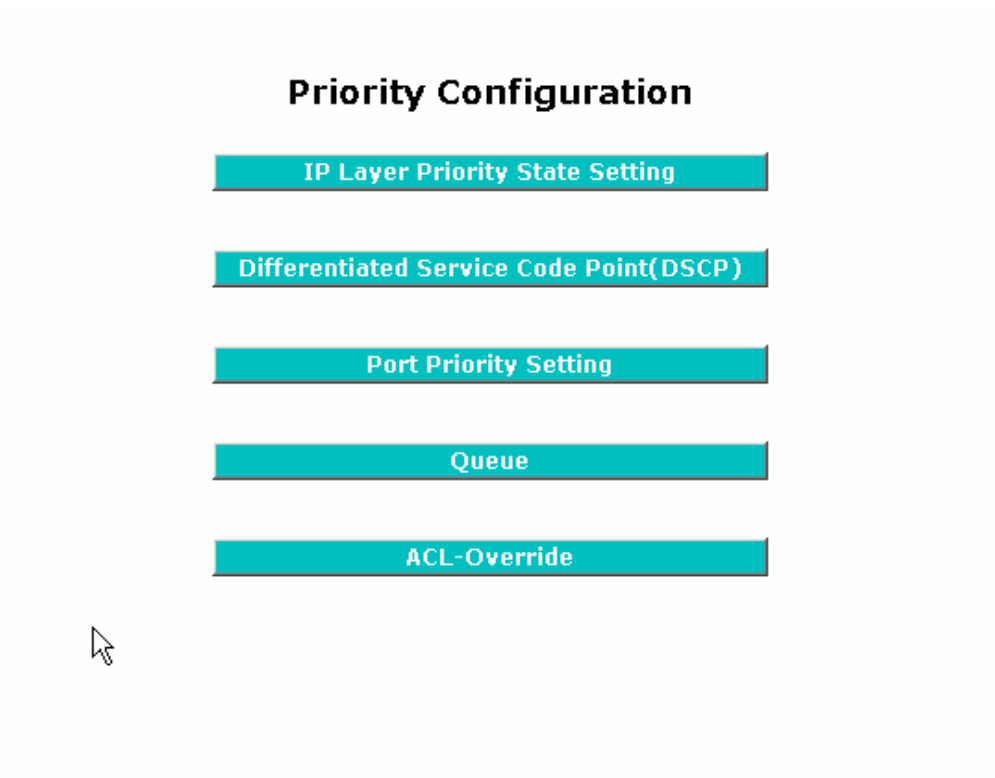



Fig. 3-13

*Function name:*

IP Layer Priority State Setting

*Function description:*

These settings could let you to disable DSCP (IP Layer) QoS effects and the effects of 802.1p or Port Priority will be taken effect. DSCP has higher precedence of influence than 802.1p and Port Priority so we need IP-ignore function to let 802.1p or Port Priority act on.

*Parameter description:*

IP-ignored:

You can choose any port as Disable or Enable state of IP-ignored. If you select port 1 as Enable state, it will disable QoS capability of DSCP.

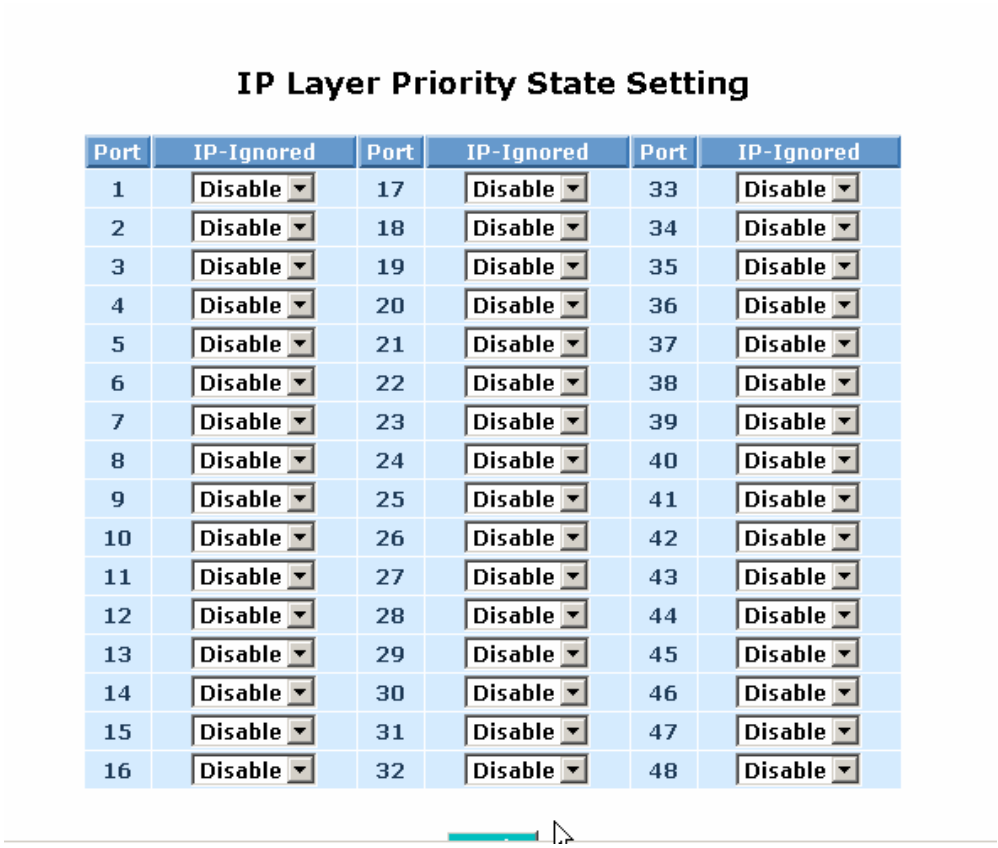

IP Layer Priority State Setting
Port IP-Ignored Port IP-Ignored Port IP-Ignored
1 Disable 17 Disable 33 Disable
2 Disable 18 Disable 34 Disable
3 Disable 19 Disable 35 Disable
4 Disable 20 Disable 36 Disable
5 Disable 21 Disable 37 Disable
6 Disable 22 Disable 38 Disable
7 Disable 23 Disable 39 Disable
8 Disable 24 Disable 40 Disable
9 Disable 25 Disable 41 Disable
10 Disable 26 Disable 42 Disable
11 Disable 27 Disable 43 Disable
12 Disable 28 Disable 44 Disable
13 Disable 29 Disable 45 Disable
14 Disable 30 Disable 46 Disable
15 Disable 31 Disable 47 Disable
16 Disable 32 Disable 48 Disable

Fig. 3-14

*Function name:*

Differentiated Service Code Point(DSCP)

*Function description:*

Differentiated Service Code Point(DSCP) function could form totally 64 (0~63) kinds of Traffic Class based on the arrangement of 6-bit field in DSCP of the IP packets. In the switch, users are allowed to set up these 64 kinds of Class that belong to any of 0~7 Priority for any DSCP. The switch supports 8 kinds of priorities and 4 Queues.

*Parameter description:*

DSCP:

Totally there are 0~63 DSCP priorities.

Priority:

You can choose any of 0~7 Priority for each DSCP.

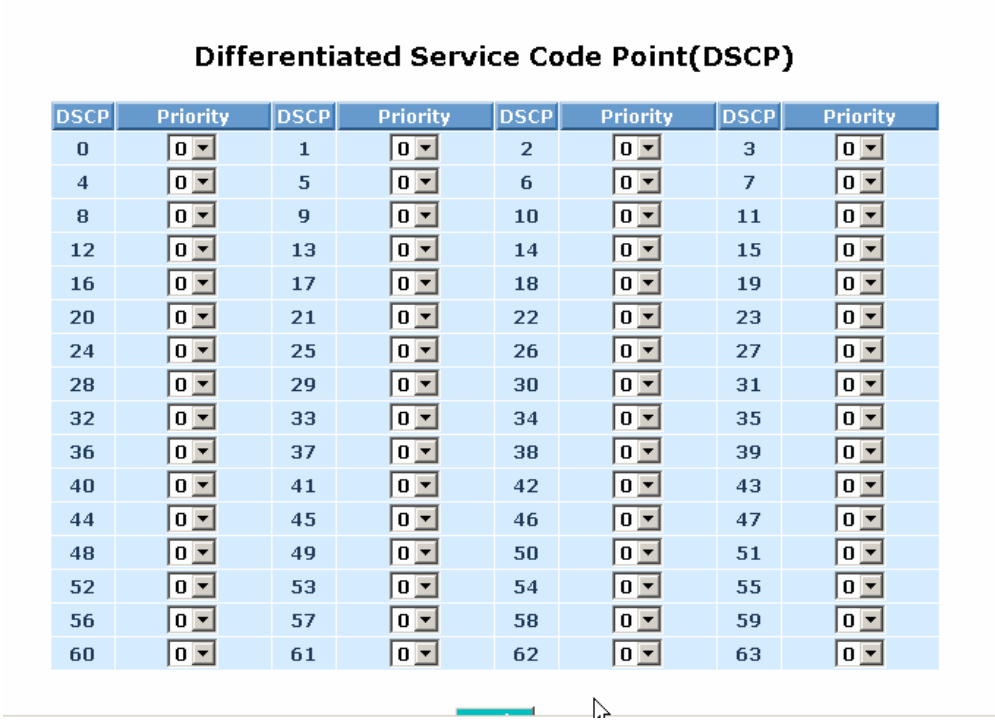



Fig. 3-15

*Function name:*

Port Priority Setting

*Function description:*

Decide the priority of each port.

*Parameter description:*

Priority:

You can choose one of 0~7 Priority for each port.

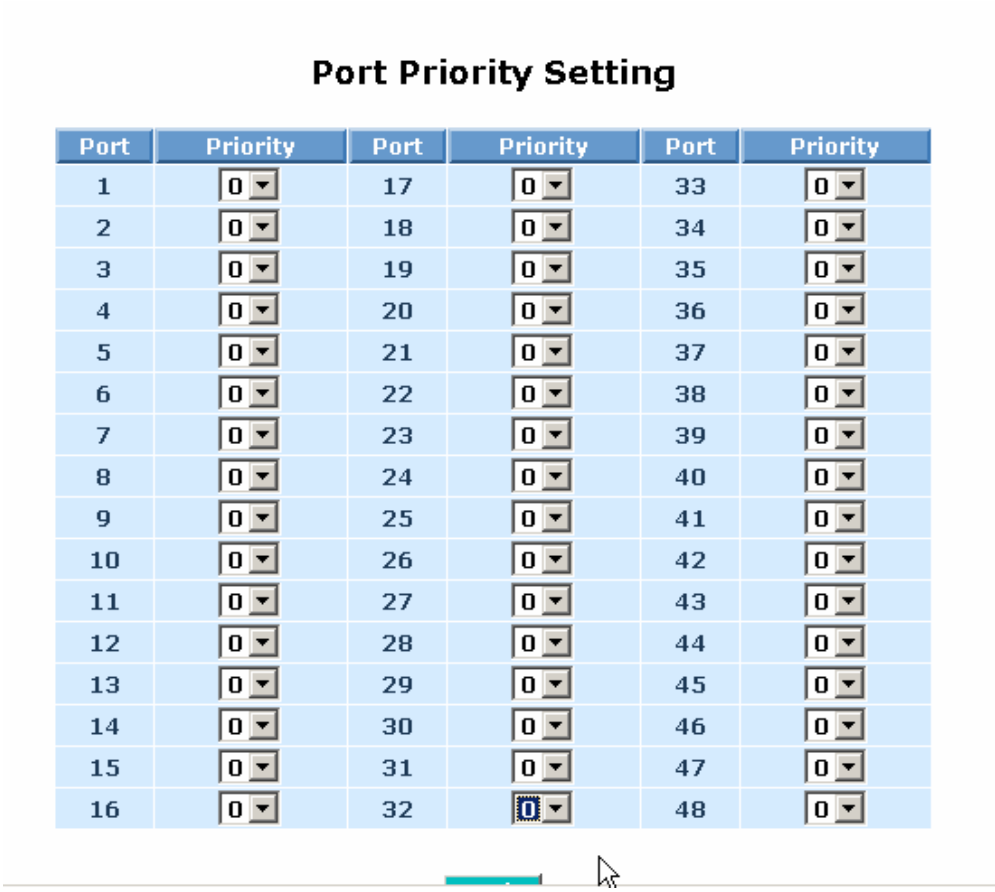



Fig. 3-16

*Function name:*

Shaper Queue

*Function description:*

The switch supports 4 Queues, 0~3, for Shaper function controlling. Any of 0~7 Priority could be mapping to any of 0~3 Queue. After determining the queue of each priority, the queue will influence of QoS scheduling and Shaper Queue when the packets transmit out from the switch. The QoS scheduling is Strict Priority. When all priorities put in the same queue, you will not see the effect of Strict Priority.

*Parameter description:*

Priority:

The switch supports 0~7 Priorities.

Queue:

You can choose any of 0~4 Queue for any of 0~7 Priority corresponding to.

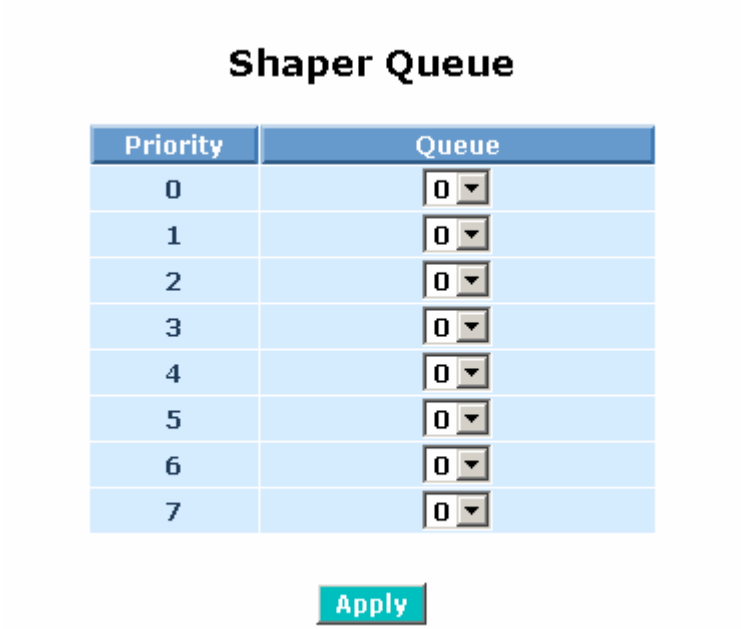



Fig. 3-17

*Function name:*

ACL Priority Override

*Function description:*

In the switch, you can let ACL priority has the higher effects of precedence for each port in ACL Priority Override function. If some ports enable ACL-Override, the other QoS priority of DSCP, 802.1P, and Priority will be seen.

*Parameter description:*

ACL-override:

You can choose Disable or Enable state of ACL-override for each port and if you choose any port as Enable state, ACL Priority will be taken effect rather other QoS priority.

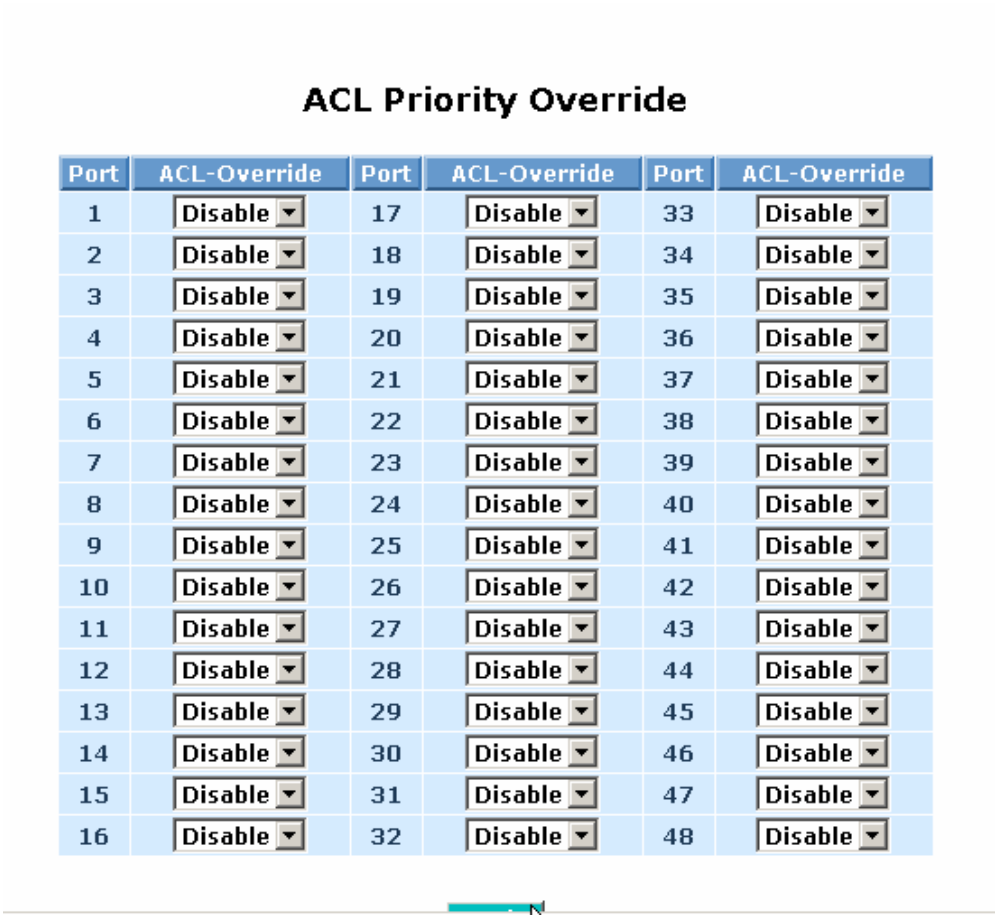

ACL Priority Override
Port ACL-Override Port ACL-Override Port ACL-Override
1 Disable 17 Disable 33 Disable
2 Disable 18 Disable 34 Disable
3 Disable 19 Disable 35 Disable
4 Disable 20 Disable 36 Disable
5 Disable 21 Disable 37 Disable
6 Disable 22 Disable 38 Disable
7 Disable 23 Disable 39 Disable
8 Disable 24 Disable 40 Disable
9 Disable 25 Disable 41 Disable
10 Disable 26 Disable 42 Disable
11 Disable 27 Disable 43 Disable
12 Disable 28 Disable 44 Disable
13 Disable 29 Disable 45 Disable
14 Disable 30 Disable 46 Disable
15 Disable 31 Disable 47 Disable
16 Disable 32 Disable 48 Disable

Fig. 3-18

### 3-6-2. Policer Configuration

*Function name:*

Policer Configuration

*Function description:*

When the packets are injected into the switch (Ingress Ports) and match Flow ID entry, Flow ID will decide which priority will be worked on by determined policer in Policer Flow ID Table. Finally, the packets will be influenced by Policer Configuration setting. Maybe the packets will be passed through or be discarded according to if the transmitting rate corresponds to the rate setting in this Policer Configuration.

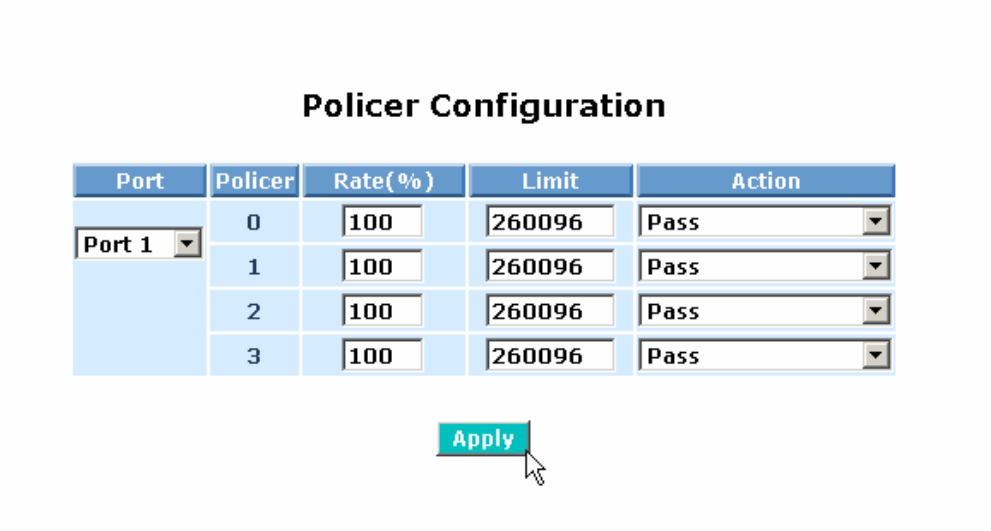



Fig. 3-19

*Parameter description:*

Port:

You can control any of 1~48 port of Policer Configuration.

Policer:

Because the switch has 4 queues, 0~3, for Ingress ports. 0~3 Policers are used for managing the 4 queues of Ingress ports in Policer Configuration.

Rate:

The rate bound and limit is for 0~3 Policer taking appropriate action. The setting range is 0~100 (%).

Limit:

The burst numbers of packets has admission to enter the switch for each Policer, It is buffer size of Ingress ports. The maximum value is 260096. The setting range is 2048~260096 (bytes). It let the switch have limiting capability of maximum packets in a flash. The feature is 260096 by default.

Action:

There are four actions for Policer Configuration using; those are Pass, Discard-congested, Discard, and Demote. “Pass” setting will let packets be entered the switch successfully on ingress ports whatever the rate is. “Discard” setting is that when the packets enter the switch and reach the rate setting in Policer Configuration function, the packets will be discarded immediately. “Discard-congested” setting is that when the rate that the packets enter the switch is reached in Policer Configuration function and the congestion happens, the packets will be discarded. “Demote” setting is referred as when the amount of packets entering the switch reaches the setting of the rate in Policer Configuration function, the priority of the packets will be decided and changed again in Mark function in QoS according to your demote’s setting and the priority of the packets when these ports enable Mark, affecting 802.1p (CoS) and DSCP. Please see Mark function in QoS capability.

### 3-6-3. Shaper Setting

*Function name:*

Shaper Setting

*Function description:*

When the packets are passed through the switch (Egress Ports) finally, the packets will put in Egress queue and be influenced by Shaper Configuration limiting rate of the packets. That the packets put in which egress queue is determined in Shaper Queue function.

*Parameter description:*

State:

To open the Shaper function with Enable state; default is Disable.

Accumulated:

The max. packets are transmitted out of the switch. The max. setting is 61440 and setting rate is 1~61440.

Port:

You can control the Shaper Setting of any of 1~48 ports .

Queue:

Each port has 4 Queue for Shaper affecting.

Rate:

Rate is the transmitting rate out of switch. The setting range is 0~100%.

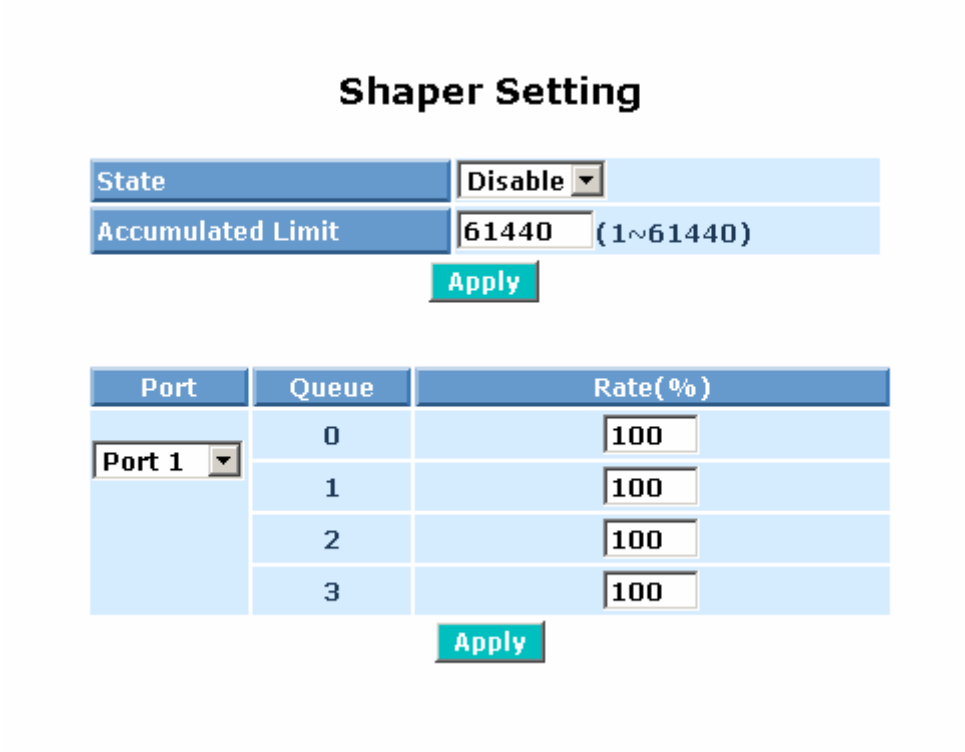

Shaper Setting
State
Disable
Accumulated Limit
61440
(1~61440)
Apply
Port
Queue
Rate(%)
Port 1
0
100
1
100
2
100
3
100
Apply

Fig. 3-20

### 3-6-4. Flow

*Function name:*

Flow

*Function description:*

When the packets enter the switch, they will be mapping to proper flow ID if they comforts to the IP Flow ID Configuration or MAC Flow ID Configuration.

And then the priorities of packets will agree with the setting in Policer Flow ID Table and are controlled by suitable policer (Policer 0~3). There are there items in Flow Setting. Those are IP Flow ID Ignore Setting, IP Flow ID Configuration and MAC Flow ID Configuration.

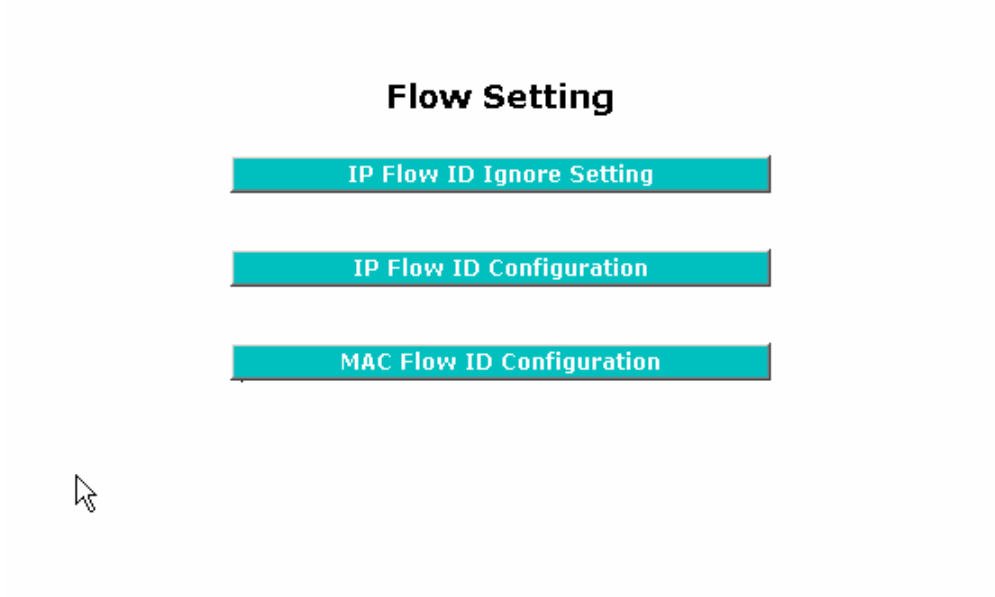



Fig. 3-21

*Function name:*

IP Flow ID Ignore Setting

*Function description:*

This section will allow you to cancel the effects of IP Flow ID and to use the influence of MAC Flow ID. When we want to make MAC Flow ID be taken effect rather IP Flow ID in some ports, you can enable IP Flow ID Ignore Setting of the ports.

*Parameter description:*

IP-ignored:

You can choose IP-ignored as Disable or Enable for each port. After selecting, press **<Apply>** button to have this function taken effect. Default is Disable.

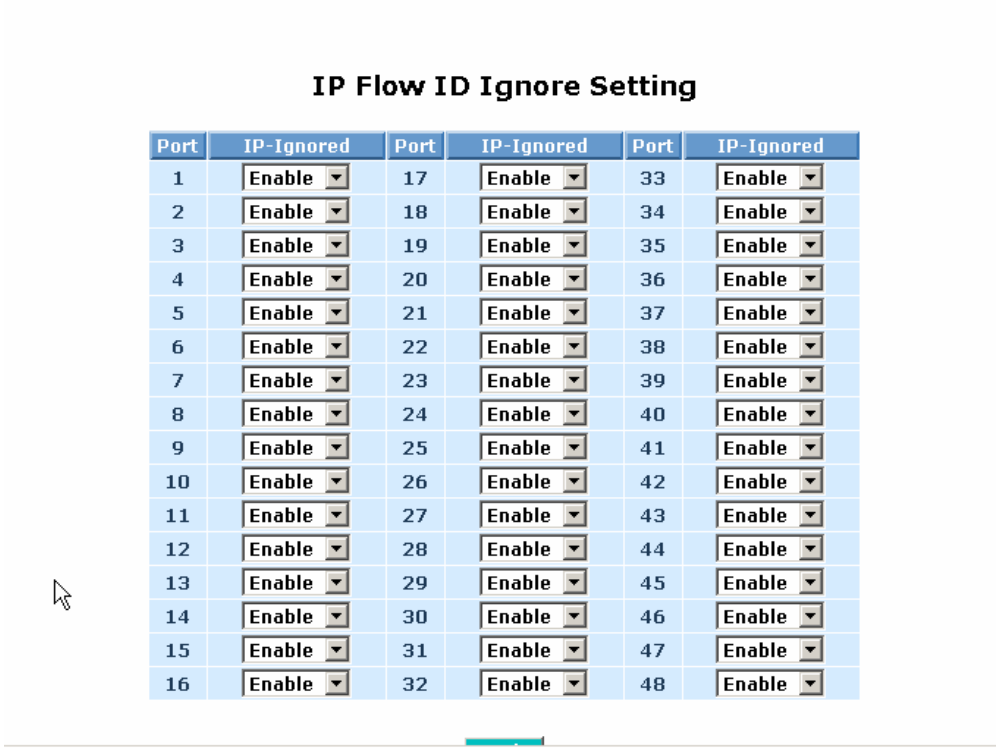

IP Flow ID Ignore Setting
Port IP-Ignored Port IP-Ignored Port IP-Ignored
1 Enable 17 Enable 33 Enable
2 Enable 18 Enable 34 Enable
3 Enable 19 Enable 35 Enable
4 Enable 20 Enable 36 Enable
5 Enable 21 Enable 37 Enable
6 Enable 22 Enable 38 Enable
7 Enable 23 Enable 39 Enable
8 Enable 24 Enable 40 Enable
9 Enable 25 Enable 41 Enable
10 Enable 26 Enable 42 Enable
11 Enable 27 Enable 43 Enable
12 Enable 28 Enable 44 Enable
13 Enable 29 Enable 45 Enable
14 Enable 30 Enable 46 Enable
15 Enable 31 Enable 47 Enable
16 Enable 32 Enable 48 Enable

Fig. 3-22

*Function name:*

IP Flow ID Configuration

*Function description:*

In IP Flow ID Configuration, click “Add” button and you will create IP Flow ID Configuration entry. When the IP packets enter the switch and fit in with the IP Flow ID Configuration, you can check Policer Flow ID Table to find which priority should be mapping to the proper policer. After IP Flow ID setting, please press **<Apply>** button in “ACL QoS Load” function to make ACL act on.

*Parameter description:*

IP:

Setting range is 0.0.0.0 ~ 255.255.255.255

Prefix:

Setting range is 1~32. If the IP packets inside IP range of IP Flow ID Configuration entry co-operating with Prefix, the packets will influenced by this IP Flow ID Configuration entry.

Source Flow ID:

Setting range is 0~3.

Destination Flow ID:

Setting range is 0~3.

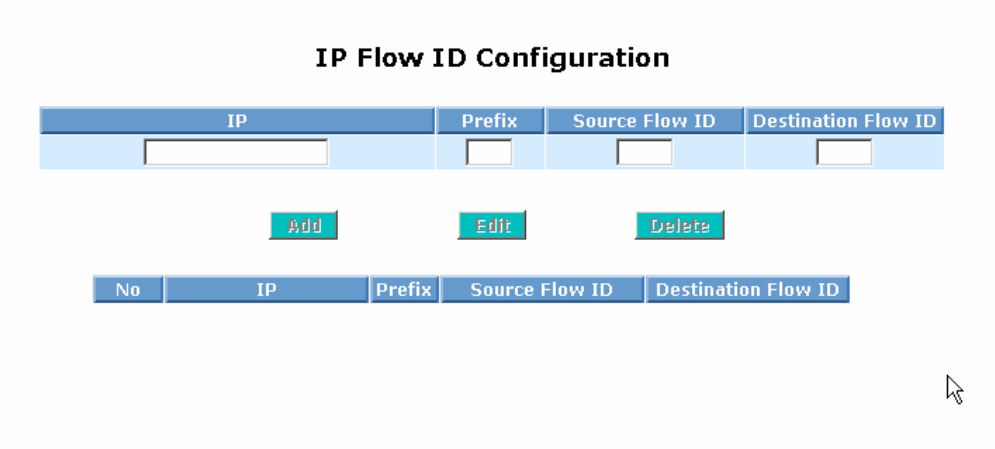



Fig. 3-23

*Function name:*

Static Forwarding MAC

*Function description:*

Click Add button and you will create MAC Flow ID Configuration entry. When the packets enter the switch and the MAC address of the packets fit in with the MAC Flow ID Configuration in some ports enabling IP Flow ID Ignore function, you can check Policer Flow ID Table to find which priority should be mapping to the proper policer. After Static Forwarding MAC setting, please press **<Apply>** button in "ACL QoS Load" function to make ACL act on.

*Parameter description:*

MAC:

Setting range is 00-00-00-00-00-00 ~ ff-ff-ff-ff-ff-fe because the mac setting must be unicast.

Port No:

Setting range is 1~48 ports.

Source Flow ID:

Setting range is 0~3.

Destination Flow ID:

Setting range is 0~3.

Alias:

You can fill any unicode.

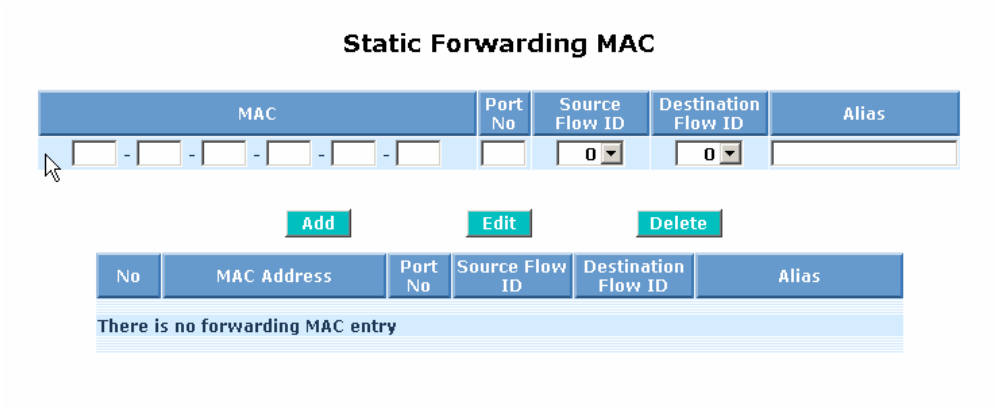



Fig. 3-24

### 3-6-5. Police-Flow

*Function name:*

Policer Flow ID Table

*Function description:*

These sections are for IP Flow ID Configuration and MAC Flow ID Configuration being mapping to and deciding appropriate Policer.

*Parameter description:*

Source Flow ID:

Setting range is 0~3. After selecting, press **<Apply>** button to have this function taken effect.

Destination Flow ID:

Setting range is 0~3. After selecting, press **<Apply>** button to have this function taken effect.

Priority:

There are 0~7 priorities totally.

Policer:

There are 0~3 Policer for each Priorities. After selecting, press **<Apply>** button to have this function taken effect.

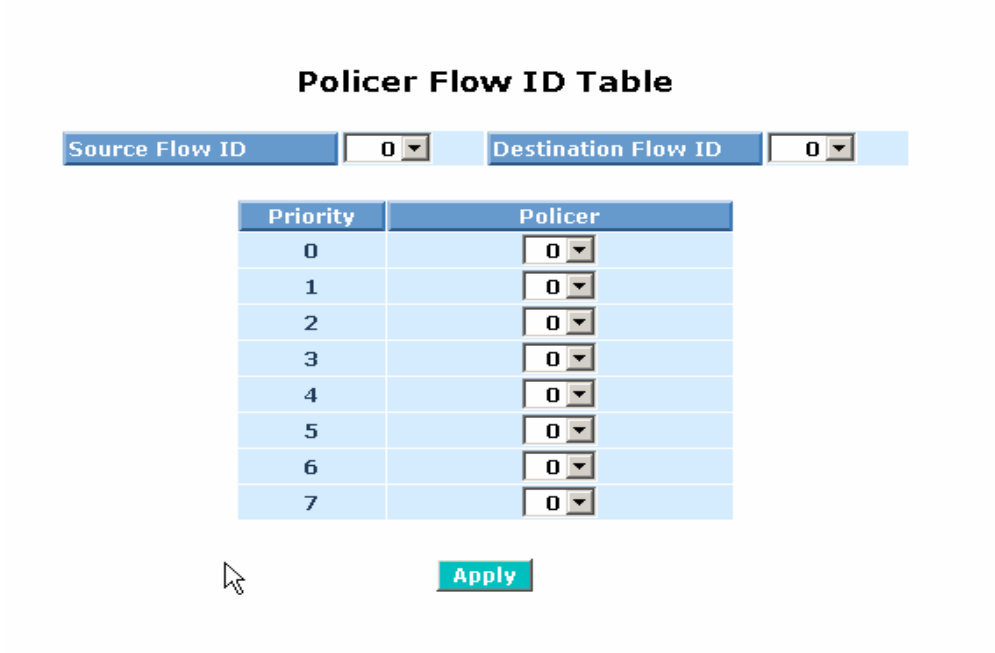



Fig. 3-25

### 3-6-6. Mark

*Function name:*

Mark Priority

*Function description:*

In Policer function in QoS, you can see the Demote capability in Action list . When the amount of packets reaches the setting of the rate and your action is determined as Demote, the queue of ingress port influenced by Policer function. The priority will be decided and changed with the setting of Demoted in Mark Priority function. Furthermore, the amount of packets doesn't reach the rate of Policer function, these packets will be put in the queues decided by your setting of Not-demoted in Mark Priority function. CoS will act on the packets of 802.1p QoS, being the priority of vlan's tag. DSCP, another's QoS capability, affects the priorities of IP Packets.

*Parameter description:*

Priority:

Totally there are 0~7 priorities in the switch..

Not-demoted:

There are 0~3 queues for your selecting in ingress ports affected by Policer function when not reaching the rate in Policer function. After selecting, press **<Apply>** button to have this function taken effect.

Demoted:

There are 0~3 queues that let you input in ingress ports affected by Policer function when reaching the rate in Policer function. After inputting setting, press **<Apply>** button to have this function taken effect.

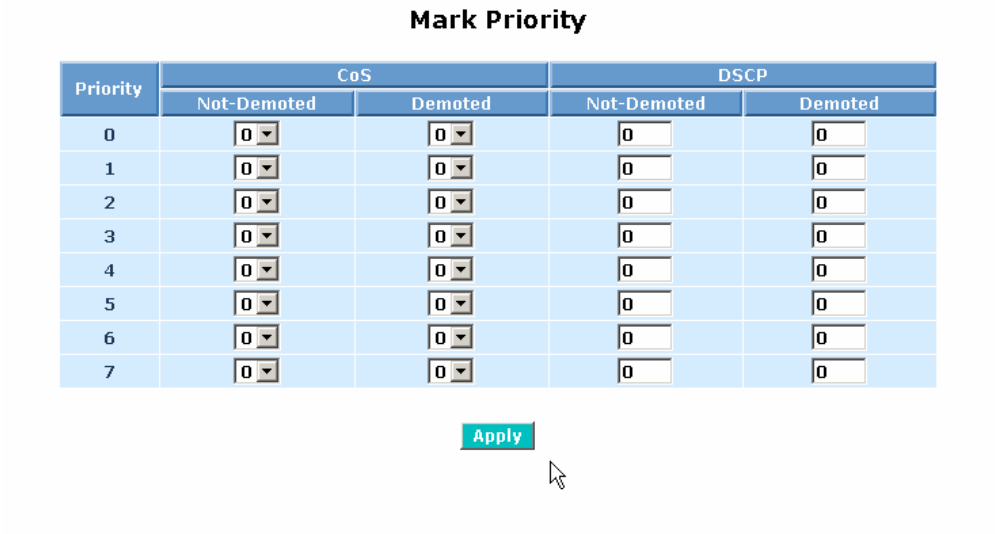

Mark Priority
Priority
CoS
DSCP
Not-Demoted
Demoted
Not-Demoted
Demoted
0
1
2
3
4
5
6
7
Apply

Fig. 3-26

### 3-6-7. Mark-enable

*Function name:*

Mark-enable CoS/DSCP

*Function description:*

You can enable the Mark function influencing on CoS/DSCP per port.

*Parameter description:*

CoS:

Make the QoS of CoS effective. There are two modes, Enable and Disable, for your selecting. After selecting, press **<Apply>** button to have this function taken effect. Default is Enable.

DSCP:

Make the QoS of DSCP effective. There are two modes, Enable and Disable, for your selecting. After selecting, press **<Apply>** button to have this function taken effect. Default is Enable.

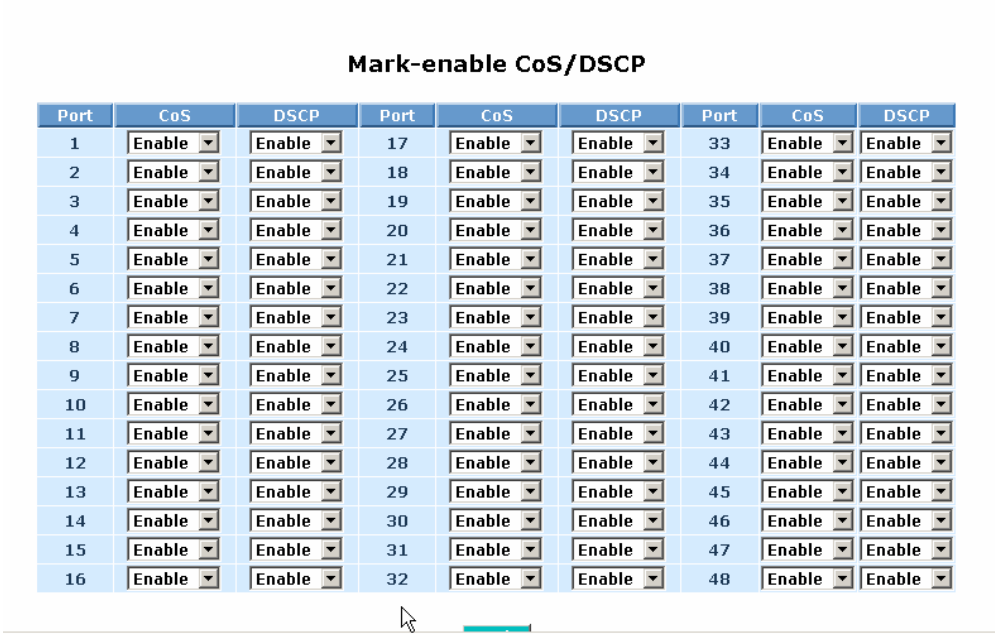

Mark-enable CoS/DSCP
Port CoS DSCP Port CoS DSCP Port CoS DSCP
1 Enable Enable 17 Enable Enable 33 Enable Enable
2 Enable Enable 18 Enable Enable 34 Enable Enable
3 Enable Enable 19 Enable Enable 35 Enable Enable
4 Enable Enable 20 Enable Enable 36 Enable Enable
5 Enable Enable 21 Enable Enable 37 Enable Enable
6 Enable Enable 22 Enable Enable 38 Enable Enable
7 Enable Enable 23 Enable Enable 39 Enable Enable
8 Enable Enable 24 Enable Enable 40 Enable Enable
9 Enable Enable 25 Enable Enable 41 Enable Enable
10 Enable Enable 26 Enable Enable 42 Enable Enable
11 Enable Enable 27 Enable Enable 43 Enable Enable
12 Enable Enable 28 Enable Enable 44 Enable Enable
13 Enable Enable 29 Enable Enable 45 Enable Enable
14 Enable Enable 30 Enable Enable 46 Enable Enable
15 Enable Enable 31 Enable Enable 47 Enable Enable
16 Enable Enable 32 Enable Enable 48 Enable Enable

Fig. 3-27

## 3-7. ACL

*Function name:*

ACL Mode

*Function description:*

ACL (Access Control List) is designed to protect the switch from unnecessary IP traffic or Layer-4 packets and allows the users to filter denial of service (DoS) floods against the switch, thereby preventing the flood from degrading the performance of the switch. You can create 64 sets of ACL. There are two mode, Port Mode and VLAN mode, for your using. In Port Mode, 48 ports use the map to same ACL number. For example, port 1 will follow to ACL number 1. However, each VLAN could choose its own ACL number in VLAN Mode. After ACL setting, please press **<Apply>** button in "ACL QoS Load" function to make ACL act on.

*Parameter description:*

ACL Mode:

There are two mode, Port Mode and VLAN mode, for your using. After selecting, press **<Apply>** button to have this function taken effect.

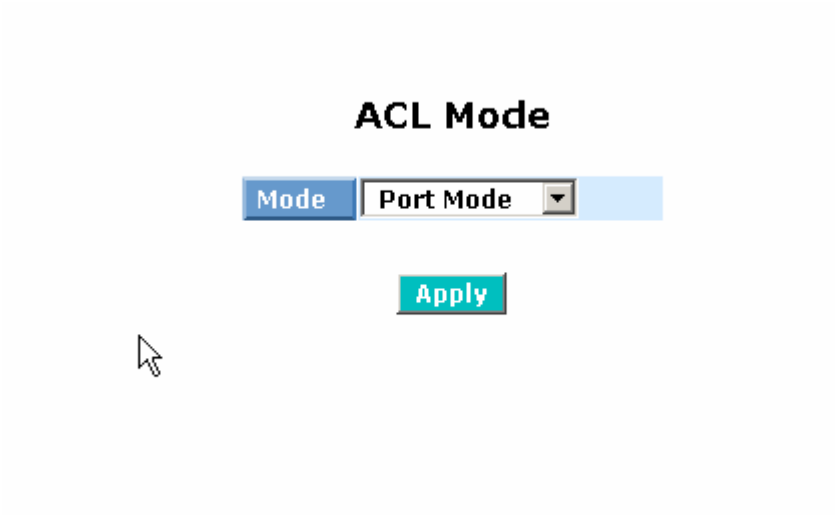



Fig. 3-28

*Function name:*

ACL/VLAN Mapping

*Function description:*

In this function, you can select the ACL number that each vlan would like be mapping to.

*Parameter description:*

VLAN ID:

This filed will appear existed VLAN VID. Default VLAN VID=1 has been created.

ACL Number:

Each VLAN ID could have 1~64 ACL Number that could be selected when you use ACL “VLAN Mode”. After selecting, press **<Apply>** button to have this function take effect.

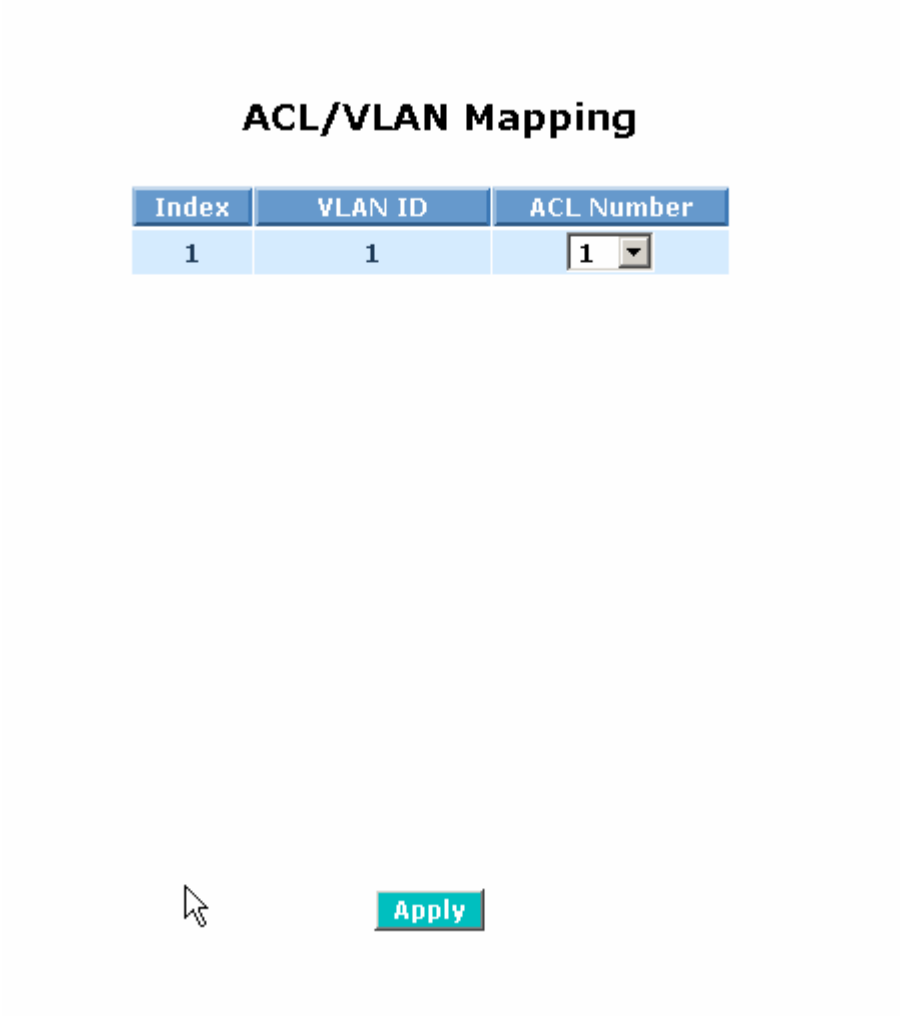



Fig. 3-29

*Function name:*

ACL Rule

*Function description:*

In this function, you can create the ACL rules in each ACL Number. The smaller index of ACL Rule will have higher effect than the higher index of ACL Rule. After ACL setting, please press **<Apply>** button in "ACL QoS Load" function to make ACL act on.

Press **<Create>** button to create ACL Rule.

Press **<Edit>** button to edit ACL Rule.

Press **<Delete>** button to delete ACL Rule.

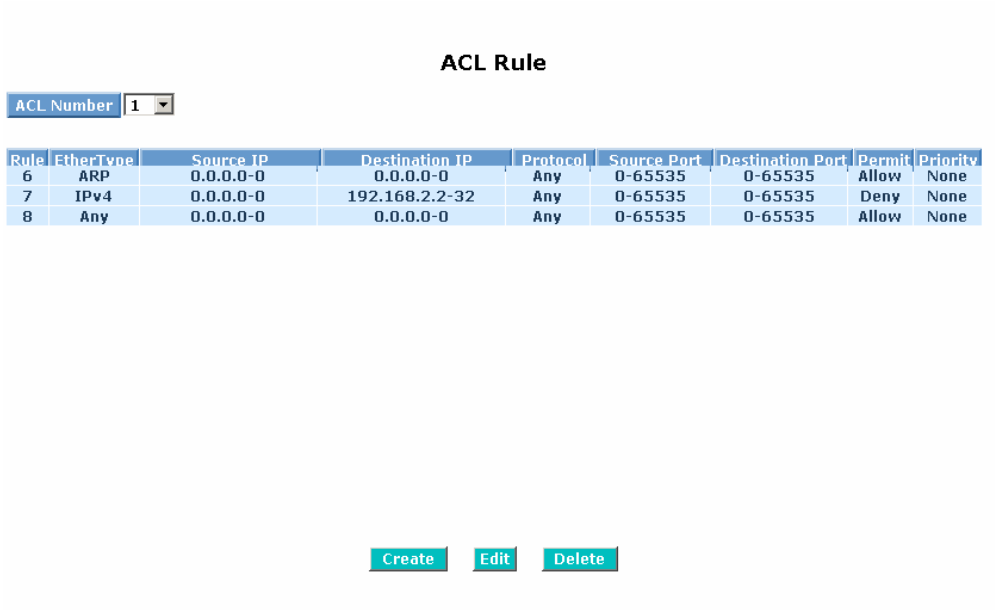

ACL Rule
ACL Number 1
Rule EtherType Source IP Destination IP Protocol Source Port Destination Port Permit Priority
6 ARP 0.0.0.0-0 0.0.0.0-0 Any 0-65535 0-65535 Allow None
7 IPv4 0.0.0.0-0 192.168.2.2-32 Any 0-65535 0-65535 Deny None
8 Any 0.0.0.0-0 0.0.0.0-0 Any 0-65535 0-65535 Allow None
Create
Edit
Delete

Fig. 3-30

*Parameter description:*

Rule:

ACL rule index.

EtherType:

Ethertype is used to indicate the protocol type in Ethernet packets and is coded as 2 bytes.

Source IP:

The Source of IP address. Range is 0.0.0.0~255.255.255.255.

Destination IP:

The Destination of IP address. Range is 0.0.0.0~255.255.255.255.

Protocol:

Protocol type in packets.

Source Port:

OSI Layer-4 Port number of Source location. Range is 0~65535.

Destination Port:

OSI Layer-4 Port number of Destination location. Range is 0~65535.

Permit:

Show if the packets could pass through or be blocked in the switch. There are two statuses, Allow or Deny.

Priority:

The transmitting precedence. If the packets conform to some ACL rule and you apply ACL QoS Load in advance , they will own this ACL priority when ACL-override enabling in QoS function. The switch supports 0~7 priority.

*Function name:*

ACL Rule Setting

*Function description:*

After pressing **<Create>** button in ACL Rule function, you will see ACL Rule Setting page. In this page, you could fill suitable setting filed and press **<Apply>** button to create ACL rule. After ACL setting, please press **<Apply>** button in "ACL QoS Load" function to make ACL act on.

*Parameter description:*

ACL:

ACL rule number. There are 1~64 ACL numbers.

Rule:

ACL rule index.

EtherType:

EtherType is used to indicate the protocol type in Ethernet packets and is coded as 2 bytes. You can select EthertType as IPv4, ARP, RARP, Type 1, Type 2, Type 3, None, or Any. Type 1,2,3 are determined by you in User Defined function.

Source IP:

The Source of IP address and IP Prefix. Range is 0.0.0.0~255.255.255.255. The range of IP Prefix is Range is 0~32.

Destination IP:

The Destination of IP address and IP Prefix. Range is 0.0.0.0~255.255.255.255. The range of IP Prefix is Range is 0~32.

Protocol:

Protocol type in packets. You can select Protocol as ICMP, IGMP, TCP, UDP, Protocol1, Protocol2, Protocol3, None, or Any. Protocol1, Protocol2, Protocol are determined by you in User Defined function.

Source Port:

OSI Layer-4 Port number of Source location would be set only when you select Protocol type as TCP OR UDP. Setting range is 0~65535.

Destination Port:

OSI Layer-4 Port number of Destination location. Setting range is 0~65535.

Permit:

Show if the packets could pass through or be blocked in the switch. There are two statuses, Allow or Deny.

Priority:

The transmitting precedence. If the packets conform to some ACL rule and you apply ACL QoS Load in advance , they will own this ACL priority when ACL-override enabling in QoS function. The switch supports 1~7 priority

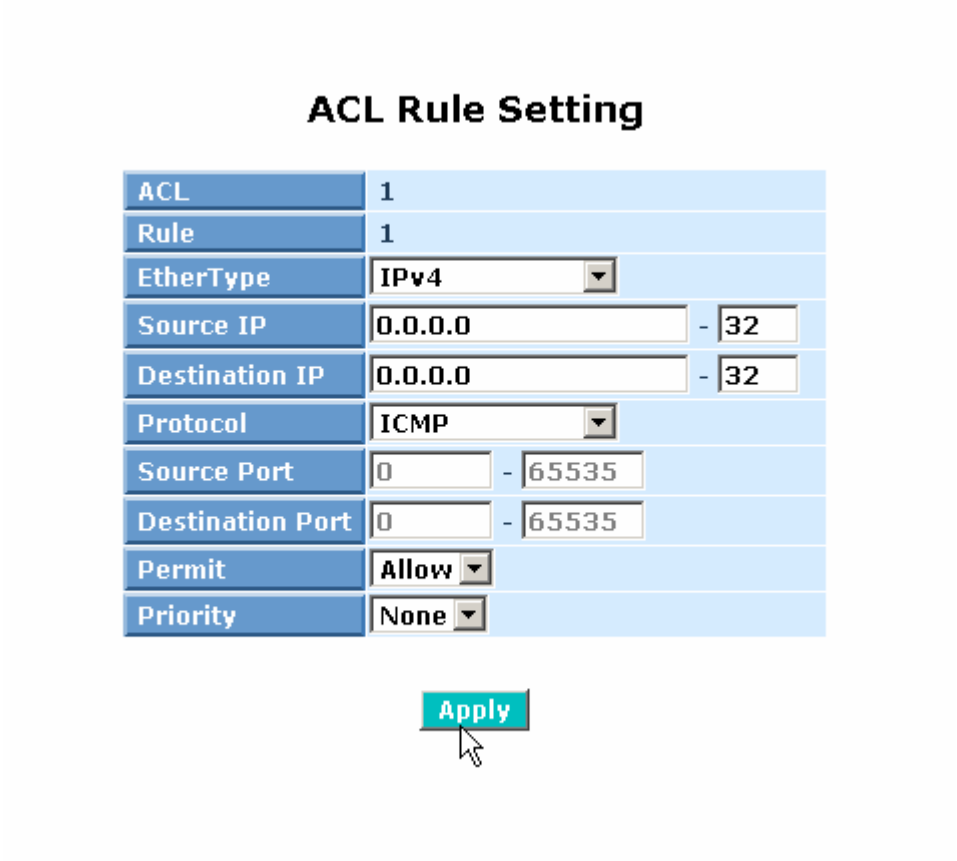



Fig. 3-31

## 3-8. ACL QoS Load

*Function name:*

ACL QoS Load

*Function description:*

Make QoS Capability in ACL function taken effect. You just press **<Apply>** button to let ACL QoS act on.

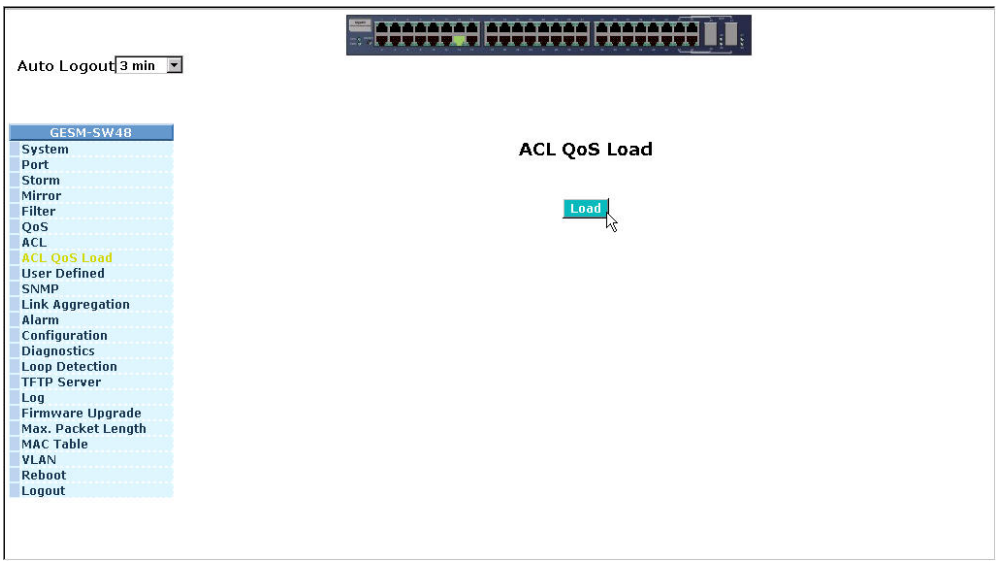



Fig. 3-32

## 3-9. User Defined

*Function name:*

User Defined

*Function description:*

Define your own values of the Ethertype and Protocol. We can find these names when creating ACL rule.

*Parameter description:*

State:

Just tick the option button to open and fill the Value of Ethertype or IP Protocol. After setting, please press **<Apply>** button to have this function taken affect.

Value:

The Value of Ethertype and IP Protocol. In Ethertype, the default is 1537; however in IP Protocol, the default is 0.

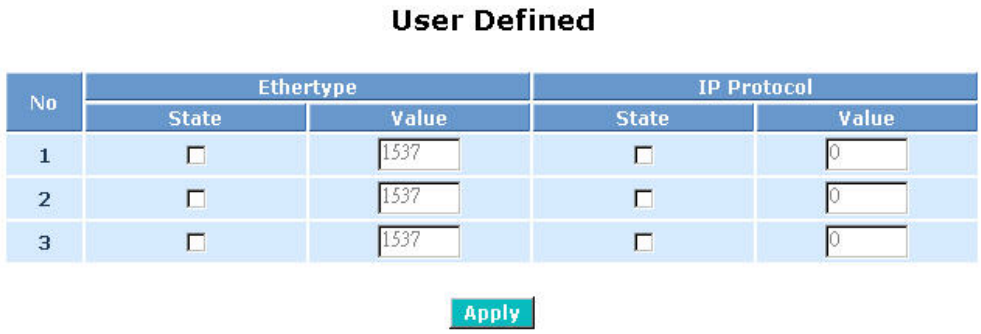



Fig. 3-33

## 3-10. SNMP Configuration

Any Network Management System (NMS) running the Simple Network Management Protocol (SNMP) can manage the Managed devices equipped with SNMP agent, provided that the Management Information Base (MIB) is installed correctly on the managed devices. The SNMP is a protocol that is used to govern the transfer of information between SNMP manager and agent and traverses the Object Identity (OID) of the management Information Base (MIB), described in the form of SMI syntax. SNMP agent is running on the switch to response the request issued by SNMP manager.

Basically, it is passive except issuing the trap information. The switch supports a switch to turn on or off the SNMP agent. If you set the field SNMP "Enable", SNMP agent will be started up. All supported MIB OIDs, including RMON MIB, can be accessed via SNMP manager. If the field SNMP is set "Disable", SNMP agent will be de-activated, the related Community Name, Trap Host IP Address, Trap and all MIB counters will be ignored.

*Function name:*

SNMP Configuration

*Function description:*

This function is used to configure SNMP settings, community name, trap host and public traps as well as the throttle of SNMP. A SNMP manager must pass the authentication by identifying both community names, then it can access the MIB information of the target device. So, both parties must have the same community name. Once completing the setting, click **<Apply>** button, the setting takes effect.

*Parameters description:*

SNMP:

The term SNMP here is used for the activation or de-activation of SNMP. Default is Enable.

Get/Set/Trap Community:

Community name is used as password for authenticating if the requesting network management unit belongs to the same community group. If they both don't have the same community name, they don't belong to the same group. Hence, the requesting network management unit can not access the device with different community name via SNMP protocol; If they both have the same community name, they can talk each other.

Community name is user-definable with a maximum length of 15 characters and is case sensitive. There is not allowed to put any blank in the community name string. Any printable character is allowable.

The community name for each function works independently. Each function has its own community name. Say, the community name for GET only works for GET function and can't be applied to other function such as SET and Trap.

Default SNMP function : Enable

Default community name for GET: public

Default community name for SET: private

Default community name for Trap: public

Default Set function : Enable

Default trap host IP address: 0.0.0.0

Default port number :162

**SNMP Configuration**

SNMP ◉ Enable ○ Disable

| No | State | Version | IP - Port | Community |
|---|---|---|---|---|
| | Security | Authentication Protocol | Authentication Password | Privacy Password |
| 1 | ☐ | v1 | - 162 | |
| | NoAuthNoPriv | MD5 | | |
| 2 | ☐ | v1 | - 162 | |
| | NoAuthNoPriv | MD5 | | |
| 3 | ☐ | v1 | - 162 | |
| | NoAuthNoPriv | MD5 | | |
| 4 | ☐ | v1 | - 162 | |
| | NoAuthNoPriv | MD5 | | |
| 5 | ☐ | v1 | - 162 | |
| | NoAuthNoPriv | MD5 | | |
| 6 | ☐ | v1 | - 162 | |
| | NoAuthNoPriv | MD5 | | |

Note : Privacy protocol always is DES

Fig. 3-34

## 3-11. Link Aggregation

The Aggregation (Port Trunking) Configuration is used to configure the settings of Link Aggregation. You can bundle more than one port with the same speed, full duplex and the same MAC to be a single logical port, thus the logical port aggregates the bandwidth of these ports. This means you can apply your current Ethernet equipments to build the bandwidth aggregation. For example, if there are three Fast Ethernet ports aggregated in a logical port, then this logical port has bandwidth three times as high as a single Fast Ethernet port has.

*Function name:*

Aggregation Configuration

*Function description:*

Display the current setup of Aggregation Trunking. With this function, user is allowed to add a new trunking group or modify the members of an existed trunking group.

Note:

Check the following to avoid errors in configuration:

When configuring the link aggregation function, you should check that whether the aggregated ports are in full-duplex mode as well as their speed is the same or not

*Parameter description:*

Port:

1~48 ports could be chosen as logical group of Link Aggregation.

Group:

It's Logical Group of Link Aggregation. There are L1~L24 for your choosing. Max. 8 ports can be selected in a logical group. Once completing the setting, click **<Apply>** button, the setting takes effect.

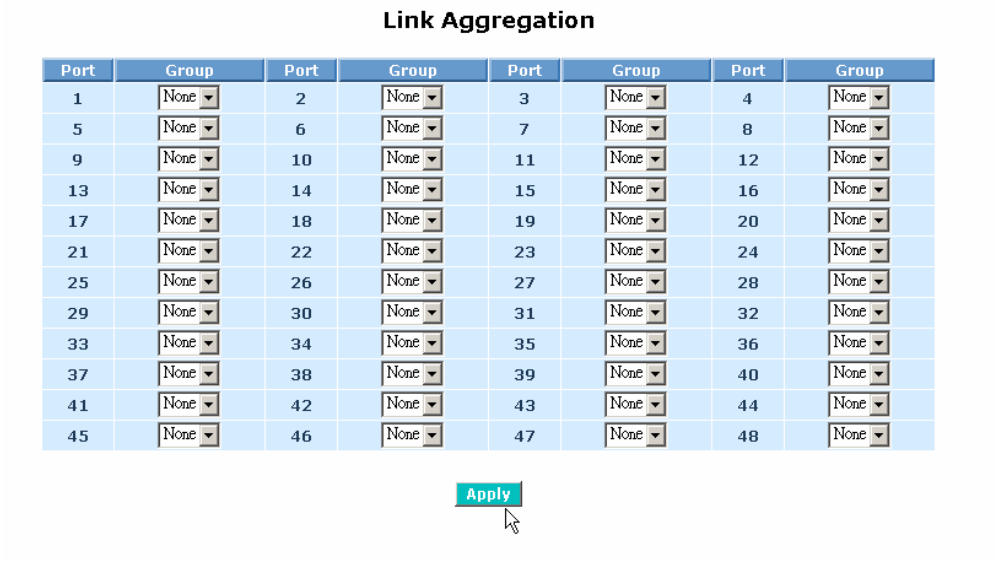
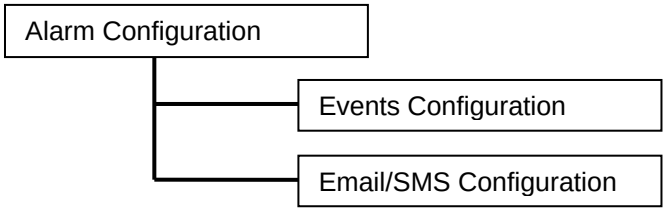

Link Aggregation
Port
Group
Port
Group
Port
Group
Port
Group
1 None 2 None 3 None 4 None
5 None 6 None 7 None 8 None
9 None 10 None 11 None 12 None
13 None 14 None 15 None 16 None
17 None 18 None 19 None 20 None
21 None 22 None 23 None 24 None
25 None 26 None 27 None 28 None
29 None 30 None 31 None 32 None
33 None 34 None 35 None 36 None
37 None 38 None 39 None 40 None
41 None 42 None 43 None 44 None
45 None 46 None 47 None 48 None
Apply

Fig. 3-35

## 3-12. Alarm Configuration




*Function name:*

Events Configuration

*Function description:*

The Trap Events Configuration function is used to enable the switch to send out the trap information while pre-defined trap events occurred. The switch offers 5 different trap events to users for switch management. The trap information can be sent out in three ways, including email, mobile phone SMS (short message system) and trap. The message will be sent while users tick (☑) the trap event individually on the web page shown as below.

*Parameter description:*

Trap: Cold Start, Warm Start, Link Down, Link Up, Authentication Failure,

**Trap Events Configuration**

| Event | Email ☐ | SMS ☐ | Trap ☐ |
|---|---|---|---|
| Cold Start | ☐ | ☐ | ☑ |
| Warm Start | ☐ | ☐ | ☑ |
| Link Down | ☐ | ☐ | ☑ |
| Link Up | ☐ | ☐ | ☑ |
| Authentication Failure | ☐ | ☐ | ☑ |

Apply

Fig. 3-36

*Function name:*

Email/SMS Configuration

*Function description:*

Alarm configuration is used to configure the persons who should receive the alarm message via either email or SMS, or both. It depends on your settings. An email address or a mobile phone number has to be set in the web page of alarm configuration (See Fig. 3-37). Then, user can read the trap information from the email or the mobile phone. This function provides 6 email addresses and 6 mobile phone numbers at most. The 5different trap events will be sent out to SNMP Manager when trap event occurs. After ticking trap events, you can fill in your desired email addresses and mobile phone numbers. Then, please click **<Apply>** button to complete the alarm configuration. It will take effect in a few seconds.

Note: SMS may not work in your mobile phone system. It is customized for different systems.

Trap:

In the switch, there are 6 trap hosts supported. Each of them has its own community name and IP address; is user-definable. To set up a trap host means to create a trap manager by assigning an IP address to host the trap message. In other words, the trap host is a network management unit with SNMP manager receiving the trap message from the managed switch with SNMP agent issuing the trap message. 6 trap hosts can prevent the important trap message from losing.

For each public trap, the switch supports the trap event Cold Start, Warm Start, Link Down, Link Up and Authentication Failure Trap. They can be enabled or disabled individually. When enabled, the corresponded trap will actively send a trap message to the trap host when a trap happens. If all public traps are disabled, no public trap message will be sent. As to the Enterprise (no. 6) trap is classified as private trap, which are listed in the Trap Alarm Configuration function folder.

Default for all public traps: Enable.

*Parameter description:*

Email:

Mail Server: the IP address of the server transferring your email.

Username: your username on the mail server.

Password: your password on the mail server.

Email Address 1 – 6: email address that would like to receive the alarm message.

SMS:

SMS Server: the IP address of the server transferring your SMS.

Username: your username in ISP.

Password: your username in ISP.

Mobile Phone 1-6: the mobile phone number that would like to receive the alarm message.

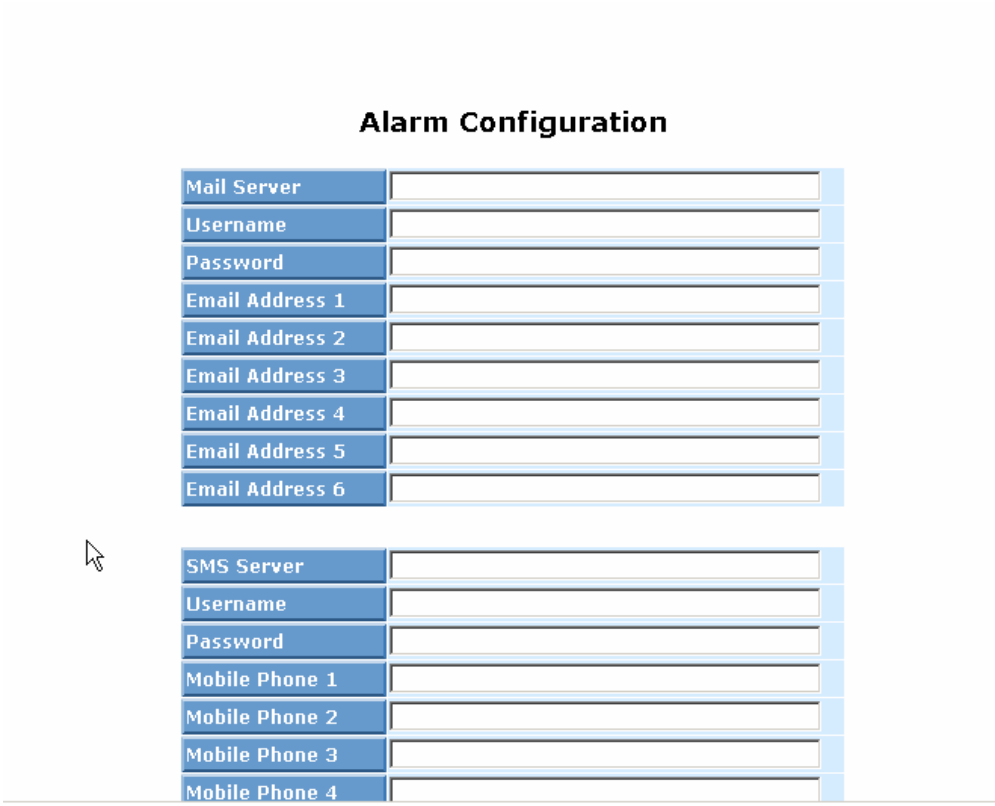



Fig. 3-37

## 3-13. Configuration

The switch supports three copies of configuration, including the default configuration, working configuration and user configuration for your configuration management. All of them are listed and described below respectively.

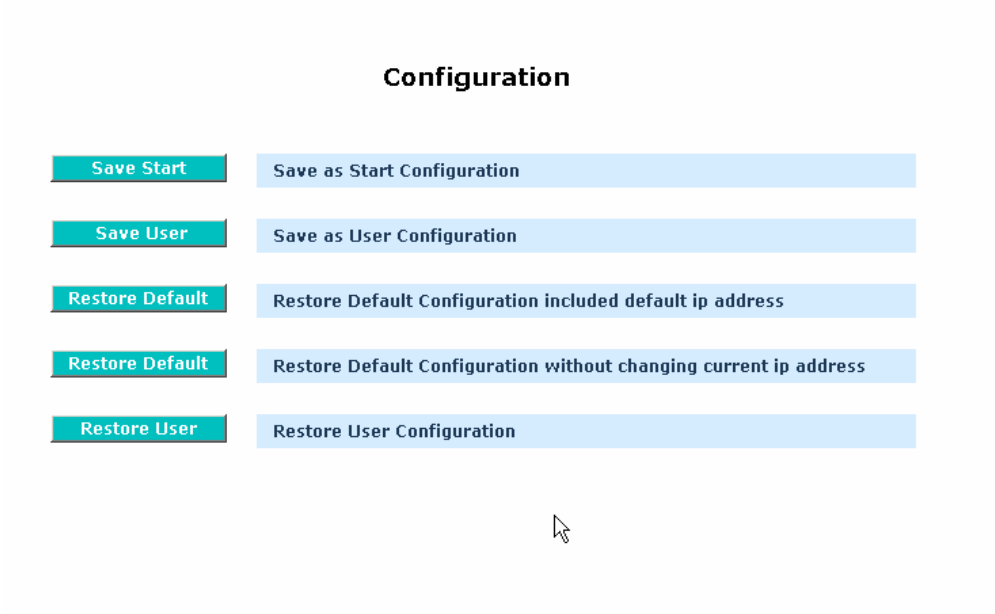



Fig. 3-38

*Function name:*

Save Start

*Function description:*

Save the current configuration as a start configuration file in flash memory.

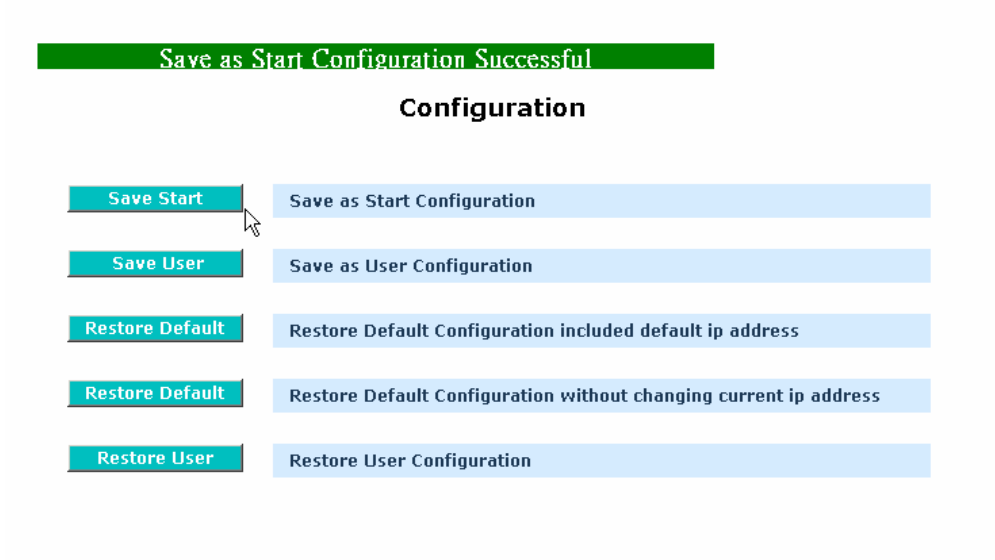



Fig. 3-39

*Function name:*

Save User

*Function description:*

Save the current configuration as a user configuration file in flash memory.

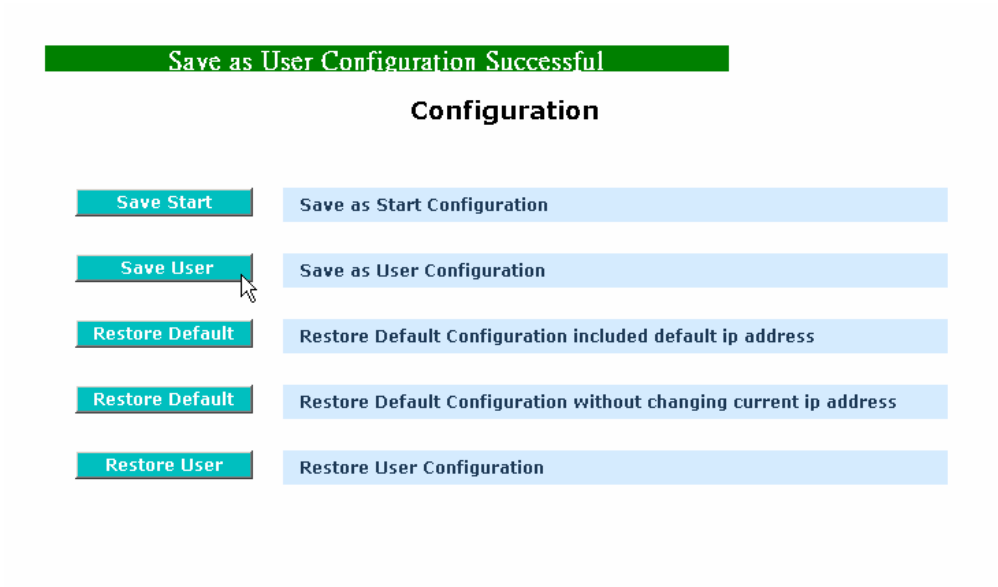



Fig. 3-40

*Function name:*

Restore Default (includes default IP address)

*Function description:*

Restore Default Configuration function can retrieve factory setting to replace the start configuration. And the IP address of the switch will also be restored to 192.168.1.1.

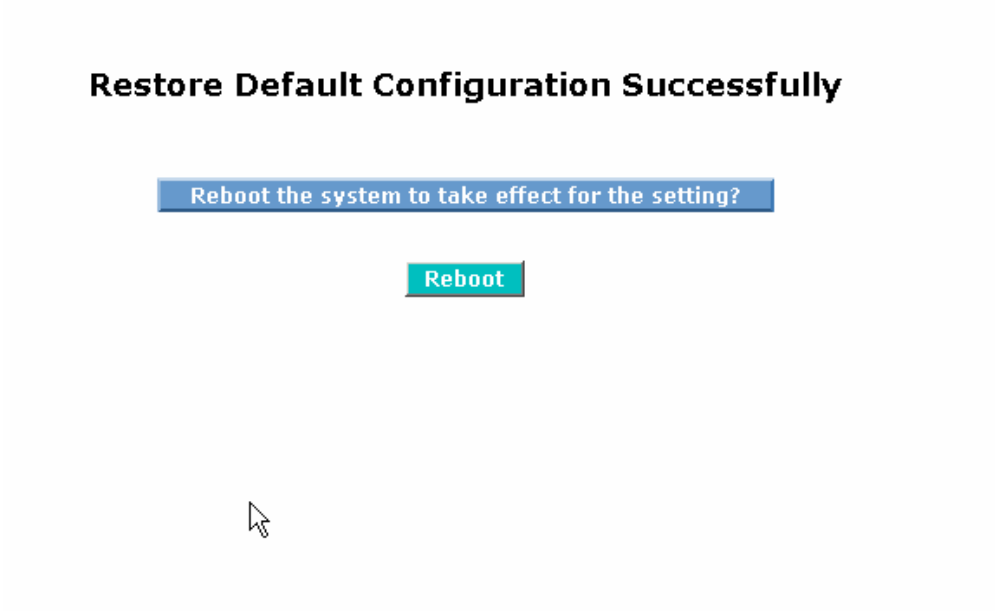



Fig. 3-41

*Function name:*

Restore Default (excludes current IP address)

*Function description:*

Restore Default Configuration function can retrieve factory setting to replace the start configuration. However, the switch's current IP address that the user set up will not be changed and will NOT be restored to 192.168.1.1 as well.

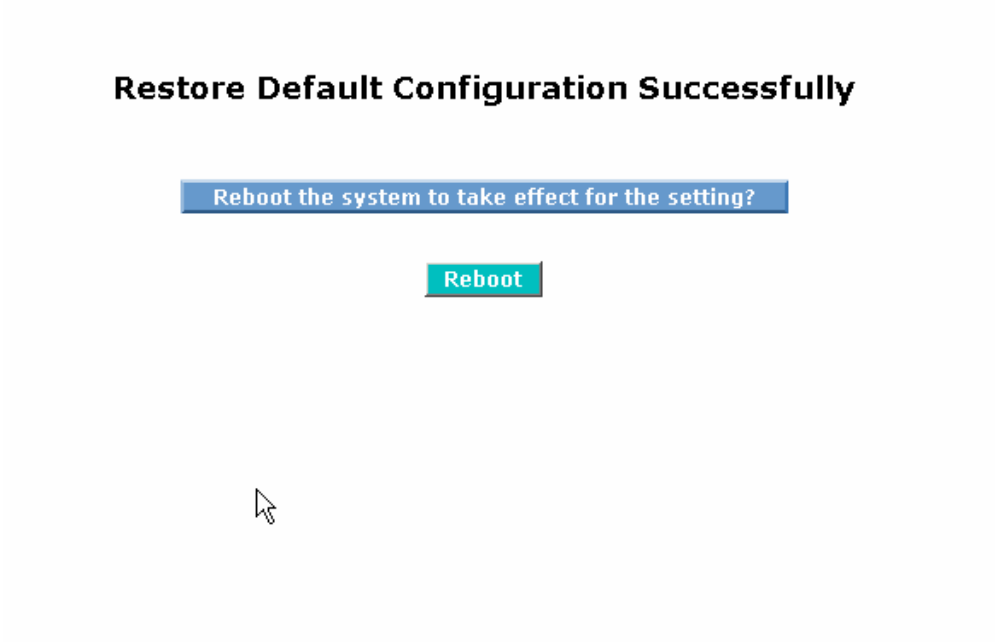



Fig. 3-42

*Function name:*

Restore User

*Function description:*

Restore User Configuration function can retrieve the previous confirmed working configuration stored in the flash memory to update start configuration. When completing to restore the configuration, the system's start configuration is updated and will be changed its system settings after rebooting the system.

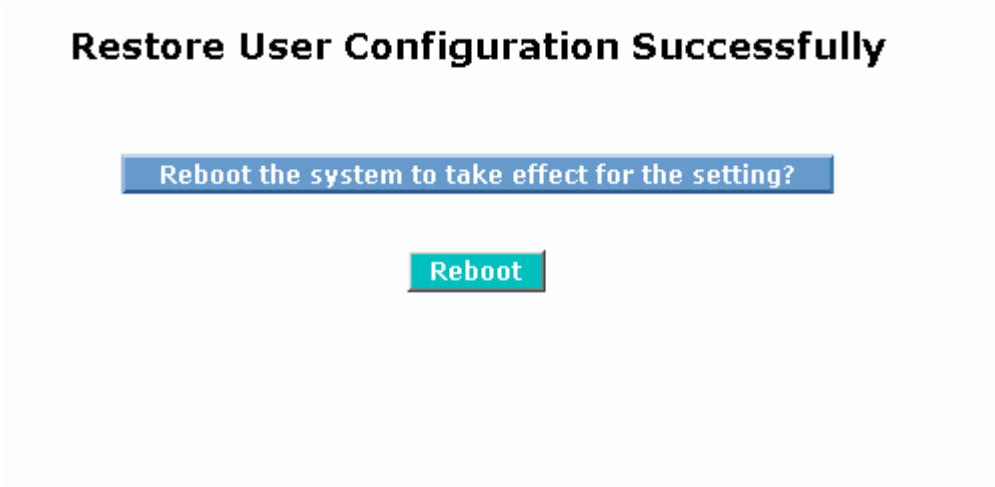
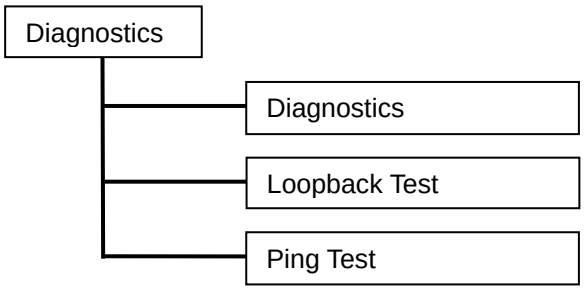



Fig. 3-43

## 3-14. Diagnostics

Three functions, including Diagnostics, Loopback Test and Ping Test are contained in this function folder for device self-diagnostics. Each of them will be described in detail orderly in the following sections.




*Function name:*

Diagnostics

*Function description:*

Diagnostics function provides a set of basic system diagnosis. It let users know that whether the system is health or needs to be fixed. The basic system check includes EEPROM test, UART test, DRAM test and Flash t

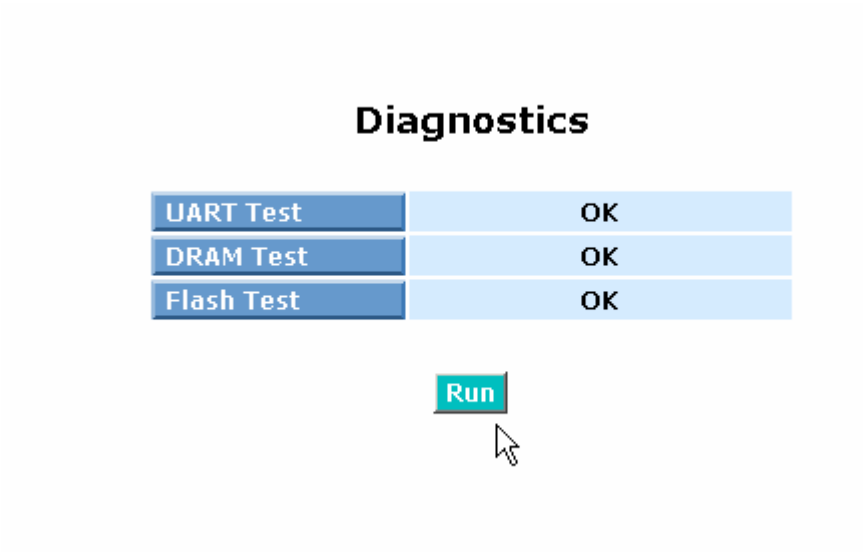



Fig. 3-44

*Function name:*

Loopback Test

*Function description:*

In the Loopback Test function, there are two different loopback tests. One is Internal Loopback Test and the other is External Loopback Test. The former test function will not send the test signal outside the switch box. The test signal only wraps around in the switch box. As to the latter test function, it will send the test signal to its link partner. If you do not have them connected to active network devices, i.e. the ports are link down, the switch will report the port numbers failed. If they all are ok, it just shows OK.

Note: Whatever you choose Internal Loopback Test or External Loopback Test, these two functions will interfere with the normal system working, and all packets in sending and receiving also will stop temporarily.

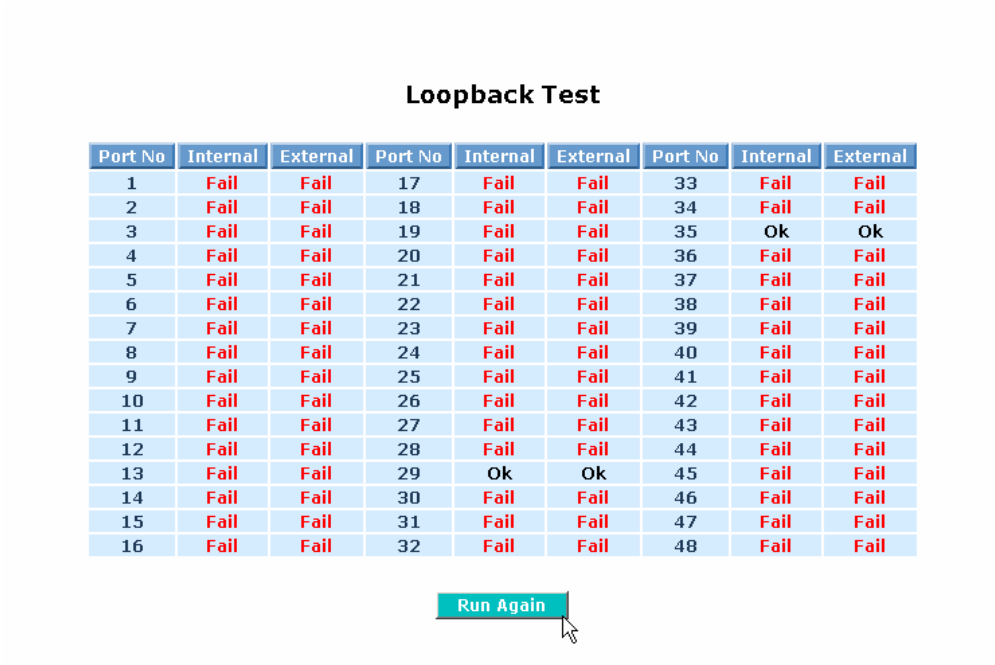

Loopback Test
Port No Internal External Port No Internal External Port No Internal External
1 Fail Fail 17 Fail Fail 33 Fail Fail
2 Fail Fail 18 Fail Fail 34 Fail Fail
3 Fail Fail 19 Fail Fail 35 Ok Ok
4 Fail Fail 20 Fail Fail 36 Fail Fail
5 Fail Fail 21 Fail Fail 37 Fail Fail
6 Fail Fail 22 Fail Fail 38 Fail Fail
7 Fail Fail 23 Fail Fail 39 Fail Fail
8 Fail Fail 24 Fail Fail 40 Fail Fail
9 Fail Fail 25 Fail Fail 41 Fail Fail
10 Fail Fail 26 Fail Fail 42 Fail Fail
11 Fail Fail 27 Fail Fail 43 Fail Fail
12 Fail Fail 28 Fail Fail 44 Fail Fail
13 Fail Fail 29 Ok Ok 45 Fail Fail
14 Fail Fail 30 Fail Fail 46 Fail Fail
15 Fail Fail 31 Fail Fail 47 Fail Fail
16 Fail Fail 32 Fail Fail 48 Fail Fail
Run Again

Fig. 3-45

*Function name:*

Ping Test

*Function description:*

Ping Test function is a tool for detecting if the target device is alive or not through ICMP protocol which abounds with report messages. The switch provides Ping Test function to let you know that if the target device is available or not. You can simply fill in a known IP address and then click **<Ping>** button. After a few seconds later, the switch will report you the pinged device is alive or dead in the field of Ping Result.

*Parameter description:*

IP Address:

An IP address with the version of v4, e.g. 192.168.1.1.

Default Gateway:

IP address of the default gateway.

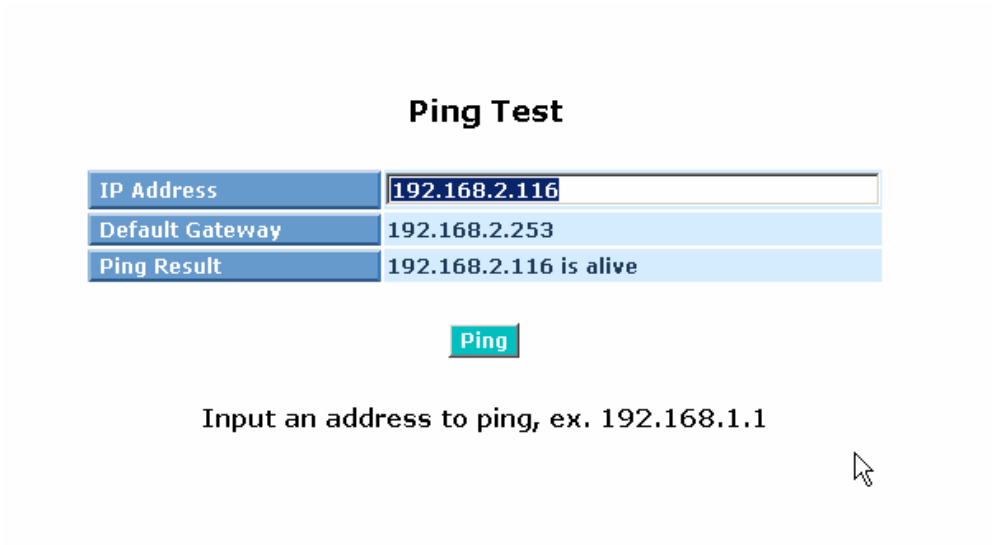



Fig. 3-46

## 3-15. Loop Detection

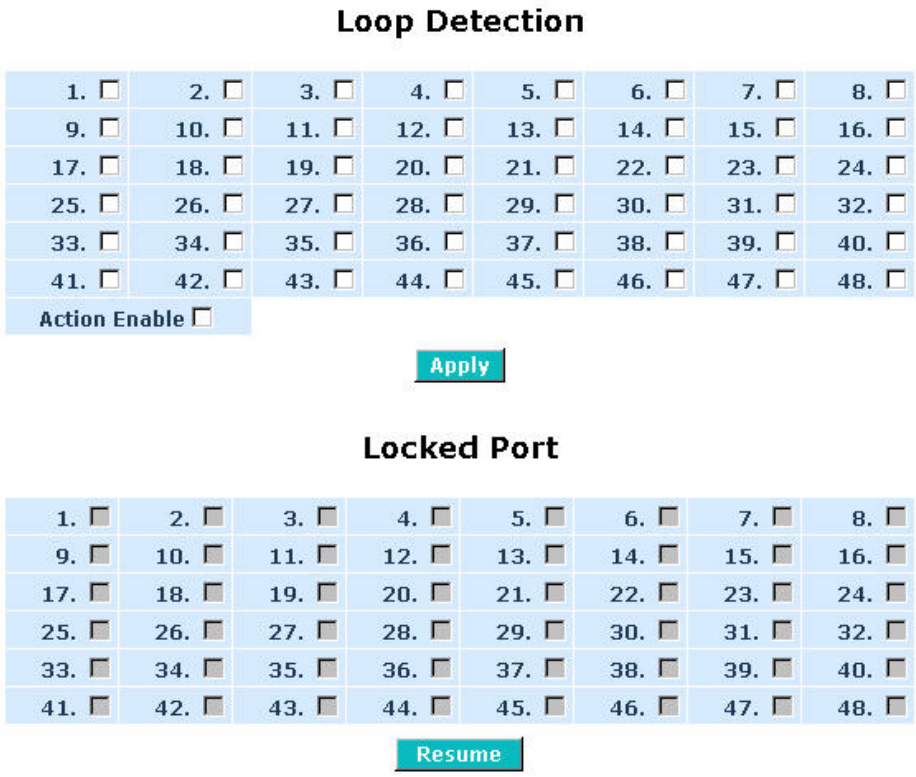



Fig. 3-47

## 3-16. TFTP Server

*Function name:*

TFTP Server

*Function description:*

Set up IP address of TFTP server.

*Parameter description:*

Specify the IP address where the TFTP server locates. Fill in the IP address of your TFTP server, then press **<Apply>** button to have the setting taken effect.

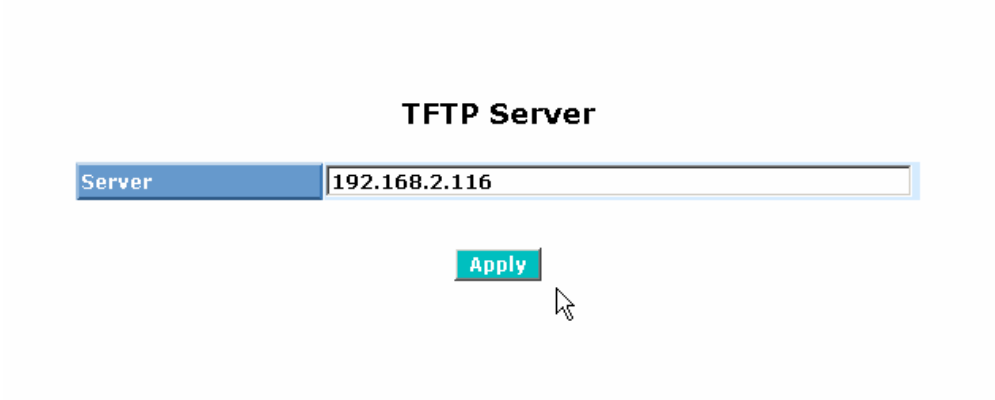



Fig. 3-48

## 3-17. Log

This function shows the log data. The switch provides system log data for users. There are 19 private trap logs, 5 public trap logs. The switch supports total 120 log entries. For more details on log items, please refer to the section of Trap/Alarm Configuration and SNMP Configuration.

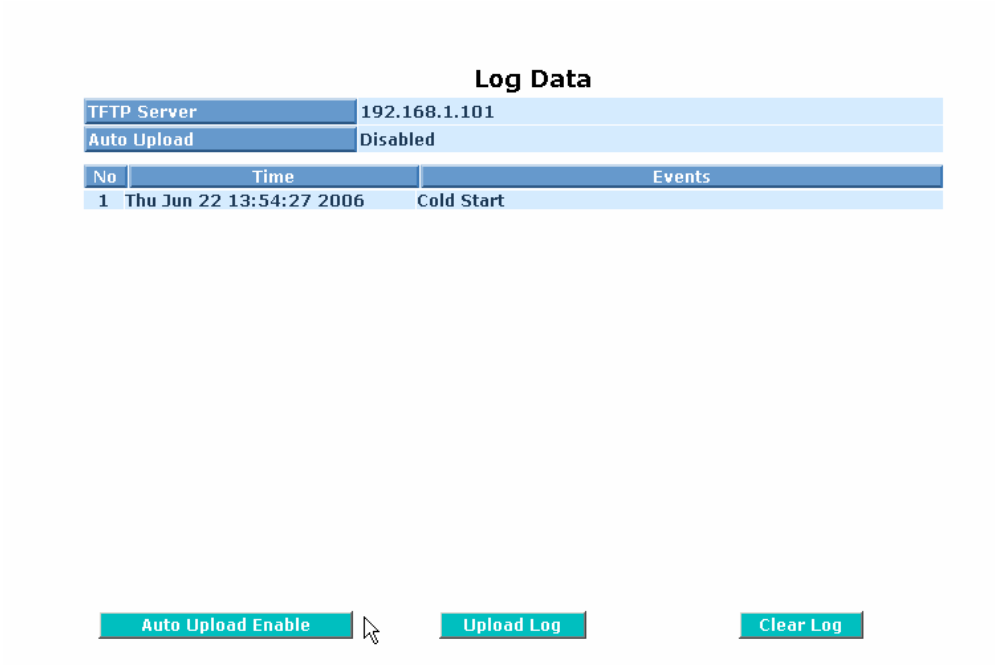



Fig. 3-49

*Function name:*

Log Data

*Function description:*

The Trap Log Data is displaying the log items including all SNMP Private Trap events, SNMP Public traps and user logs occurred in the system. In the report table, No., Time and Events are three fields contained in each trap record.

*Parameter description:*

TFTP Server:

TFTP Server IP address. Log upload must co-operate with TFTP server.

Auto Upload:

Auto Upload Status.

No.:

Display the order number when the trap happened.

Time:

Display the time when the trap happened.

Events:

Display the trap event name.

Auto Upload Enable:

Switch the enabled or disabled status of the auto upload function.

Upload Log:

Upload log data through TFTP.

Clear Log:

Clear log data.

## 3-18. Firmware Upgrade

Software upgrade tool is used to help upgrade the software function in order to fix or improve the function. The switch provides a TFTP client for software upgrade. This can be done through Ethernet.

*Function name:*

Firmware Upgrade

*Function description:*

The switch supports TFTP upgrade tool for upgrading software. If you assure to upgrade software to a newer version one, you must follow two procedures:

1.) Specifying the IP address where TFTP server locates. In this field, the IP address of your TFTP server should be filled in.

2.) Specifying what the filename and where the file is. You must specify full path and filename.

Then, press **<Upgrade>** button if your download is not successful, the switch will also be back to “Software Upgrade”, and it will not upgrade the software as well.

When download is completed, the switch starts upgrading software. A reboot message will be prompted after completing upgrading software. At this time, you must reboot the switch to have new software worked.

Note: Software upgrade is hazardous if power is off. You must do it carefully.

*Parameter description:*

TFTP Server: A TFTP server stored the image file you want to upgrade.

Path and Filename: File path and filename stored the image file you want to upgrade.

Fig. 3-50

## 3-19. Max. Packet Length

*Function name:*

Maximum Packet Length Configuration

*Function description:*

The switch is capable of dealing with Jumbo Frames of 16k length, which suit the transmission for a large amount of data in the network environment.

*Parameter description:*

Maximum (bytes):

Set up the maximum length of the packet to let each port of the switch can accept. Maximum length can be up to 16383 bytes. The default is 1522 bytes.

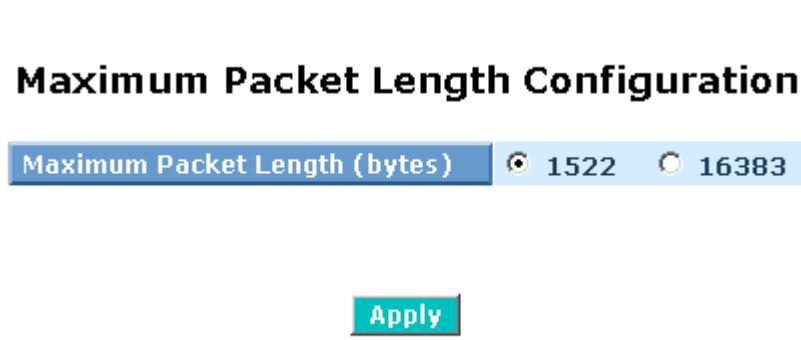



Fig. 3-51

## 3-20. MAC Table

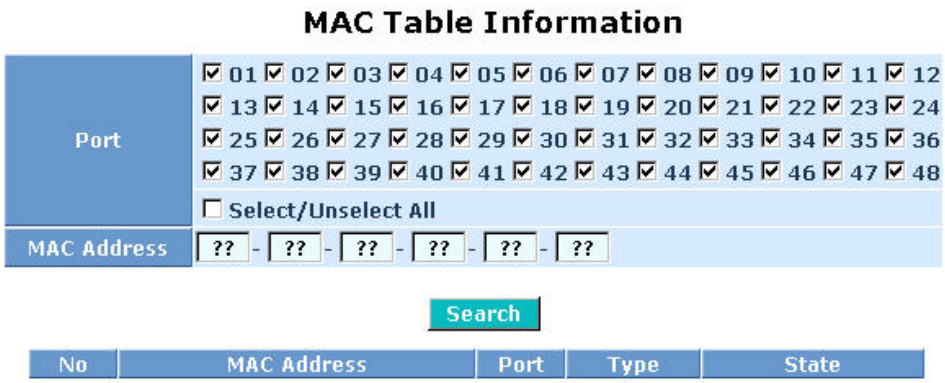



Fig. 3-52

Fig. 3-53

*Function Name:*

Static Forwarding MAC

*Function Description:*

Static Forward is a function allowing the user to create the static forward table to access a specified port of the switch. Static Forward table associated with a specified port of a switch is set up by manually inputting MAC address and its alias name.

When a MAC address is assigned to a specific port, all of the switch's traffics with this MAC address could be forwarded through this port of the switch.

For adding a MAC address entry in the allowed table, you just need to fill in four parameters: MAC address, associated port, and Alias. Just select the existed MAC address entry of your wanting and click **<Delete>** button, you also can remove it.

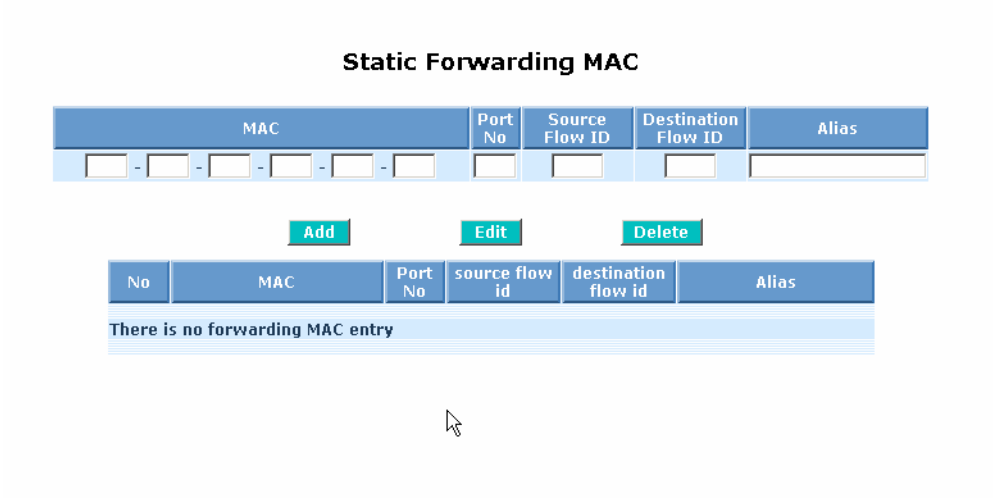



Fig. 3-54

*Parameter description:*

MAC:

It is a six-byte long Ethernet MAC address and usually expressed by hex and separated by hyphens. For example,

00 – 40 - C7 - D6 – 00 - 01

Port No:

Port number of the switch. It is 1 ~48.

Source Flow ID:

The setting range is 0~3 and is influenced by Flow ID setting in QoS.

Destination Flow ID:

The setting range is 0~3 and is influenced by Flow ID setting in QoS.

Alias:

MAC alias name for your assigning.

*Function Name:*

Static Filtering MAC

*Function Description:*

Static Filter is a function denying the packet forwarding through the switch if the packet's MAC Address is listed in the filtering Static Filter table. User can very easily maintain the table by filling in MAC Address, and Alias fields individually. User also can delete the existed entry by clicking **<Delete>** button.

*Parameter description:*

MAC:

It is a six-byte long MAC hardware address and usually expressed by hex and separated by hyphens. For example,

00 – 40 - C7 - D6 – 00 - 02

Alias:

MAC alias name for your assigning.

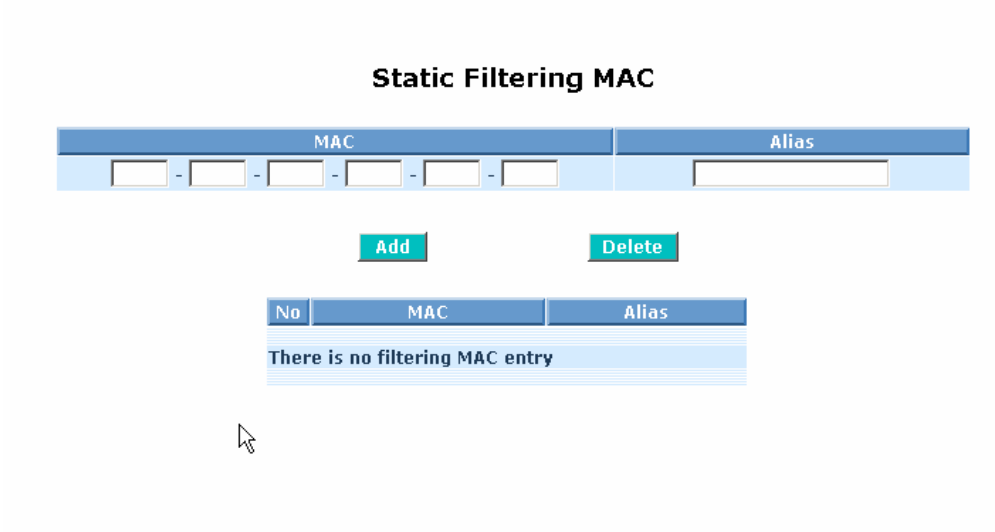



Fig. 3-55

## 3-21. VLAN

### 3-21-1. VLAN Mode

*Function name:*

VLAN Mode

*Function description:*

The VLAN Mode Selection function includes two modes: Port-based and Tag-based, you can choose one of them by pulling down the list items and selecting an item. Default is Tag-based. Then, click **<Apply>** button, the settings will take effect immediately.

Fig. 3-56

*Parameter description:*

VLAN Mode:

Port-based:

Port-based VLAN acts according the port group. Any packet transmit in or out in the same group of a port-based VLAN of the switch. For example, for a port-based VLAN named PVLAN-1 contains port members Port 1&2&3&4. If you are on the port 1, you can communicate with port 2&3&4. If you are on the port 5, then you cannot talk to PVLAN-1. Each port-based VLAN must be assigned a group name. This switch can support up to maximal 72 port-based VLAN groups.

Tag-based:

Tag-based VLAN identifies its member by VID. This is quite

different from port-based VLAN. If there are any rules in ingress filtering list or egress filtering list, the packet will be screened with more filtering criteria to determine if it can be forwarded.

Each tag-based VLAN must be assigned VLAN name and VLAN ID. Valid VLAN ID is 1-4094. User can create total up to 256 Tag VLAN groups.

### 3-21-2. VLAN Group

*Function name:*

Tag-based VLAN

*Function description:*

It shows the information of existed Tag-based VLAN Groups, You can also easily create, edit and delete a Tag-based VLAN group by pressing **< Create VLAN >**, **<Edit VLAN>** and **<Delete VLAN>** function buttons. Users can add a new VLAN group by inputting a new VLAN name and VLAN ID. In the switch, logical ports also could be created as VLAN group. Logical Ports are according to the configuration of Link Aggregation that could create 24 sets of logical ports of Link Aggregation.

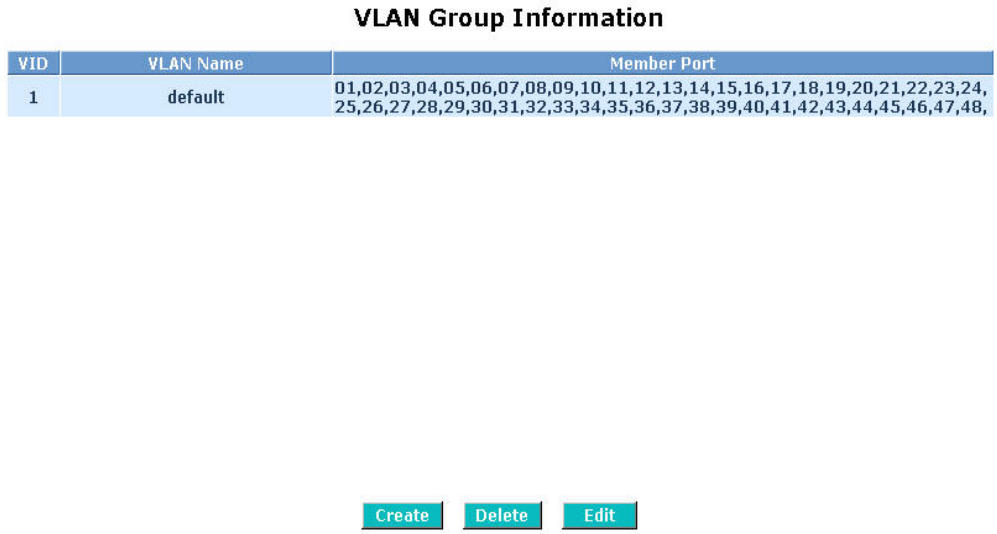



Fig. 3-57

*Parameter description:*

VLAN Name:

The name defined by administrator is associated with a VLAN group. Valid letters are A-Z, a-z, 0-9, " - " and "_" characters. The maximal length is 15 characters.

VLAN ID:

VLAN identifier. Each tag-based VLAN group has a unique VID. It appears only in tag-based and Double-tag mode.

Member Port:

This is used to enable or disable if a port is a member of the new added VLAN, “Enable” means it is a member of the VLAN. Just tick the check box (☑) beside the port x to enable it. Port-based VLAN group could include physical ports (1~48 ports) or logical ports (1~24).

Create VLAN:

Create a new Tag-based VLAN. Input the VLAN name and choose the member by ticking the check box beside the port No., then, press the **<Apply>** button to have the setting taken effect.

Delete VLAN:

Just press the **<Delete VLAN>** button to remove the selected group entry from the Tag-based group table.

Edit VLAN:

Just select a group entry and press the **<Edit VLAN>** button, then you can modify a group‘s description and member set.

All Port Unchecked:

Check box (☑) of all member ports will become unchecked after “All Port Unchecked”.

All Port Checked:

All uncheck box of all member ports will become checked (☑) after “All Port Checked”.

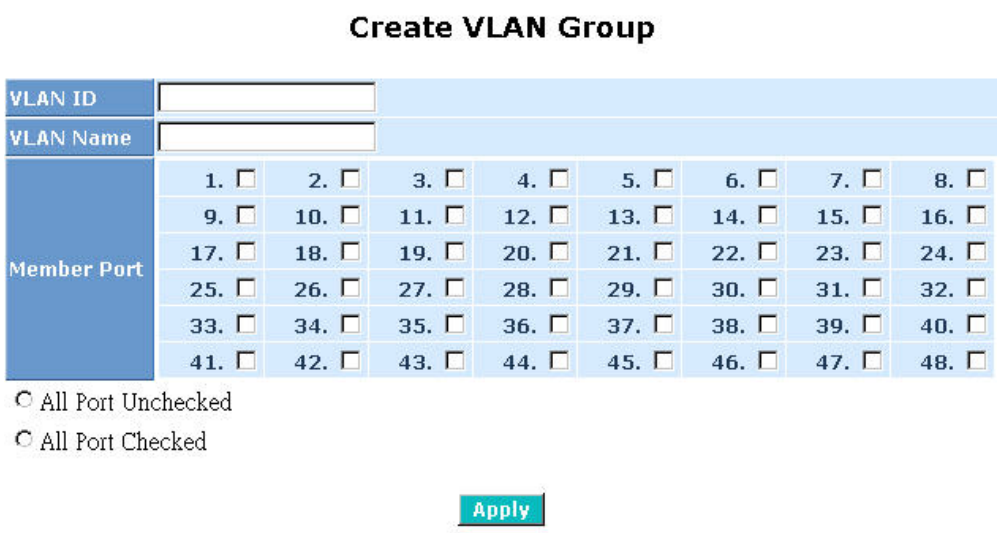



Fig. 3-58

*Function name:*

Port-based VLAN

*Function description:*

It shows the information of the existed Port-based VLAN Groups. You can easily create, edit and delete a Port-based VLAN group by pressing **<Create VLAN >**, **<Edit VLAN>** and **<Delete VLAN>** function buttons. Users can add a new VLAN group by inputting a new VLAN name. In the switch, logical ports also could be created as VLAN group. Logical Ports are according to the configuration of Link Aggregation that could create 24 sets of logical ports of Link Aggregation.

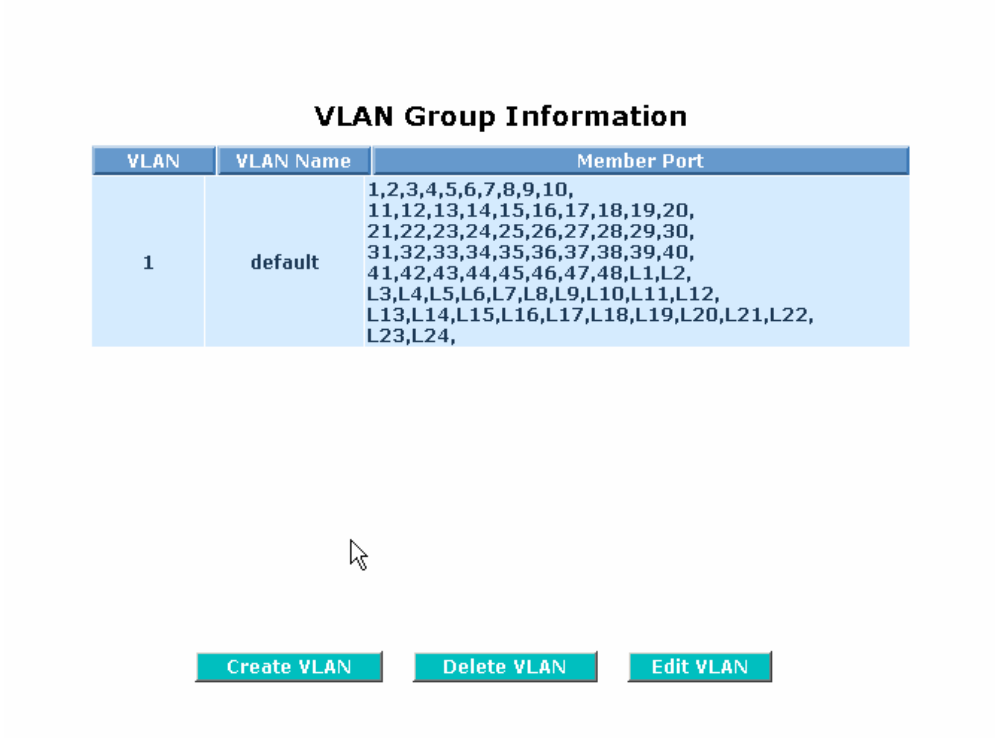



Fig. 3-59

*Parameter description:*

VLAN Name:

The name defined by administrator is associated with a VLAN group. Valid letters are A-Z, a-z, 0-9, " - " and "_" characters. The maximal length is 15 characters.

VLAN:

VLAN group index.

Member Port:

This is used to enable or disable if a port is a member of the new added VLAN, “Enable” means it is a member of the VLAN. Just tick the check box (☑) beside the port x to enable it. Port-based VLAN group could include physical ports (1~48 ports) or logical ports (1~24).

Create VLAN:

Create a new Port-based VLAN. Input the VLAN name and choose the member by ticking the check box beside the port No., then, press the **<Apply>** button to have the setting taken effect.

Delete VLAN:

Just press the **<Delete VLAN>** button to remove the selected group entry from the Port-based group table.

Edit VLAN:

Just select a group entry and press the **<Edit VLAN>** button, then you can modify a group‘s description and member set.

All Port Unchecked:

Check box (☑) of all member ports will become unchecked after “All Port Unchecked”.

All Port Checked:

All uncheck box of all member ports will become checked (☑) after “All Port Checked”.

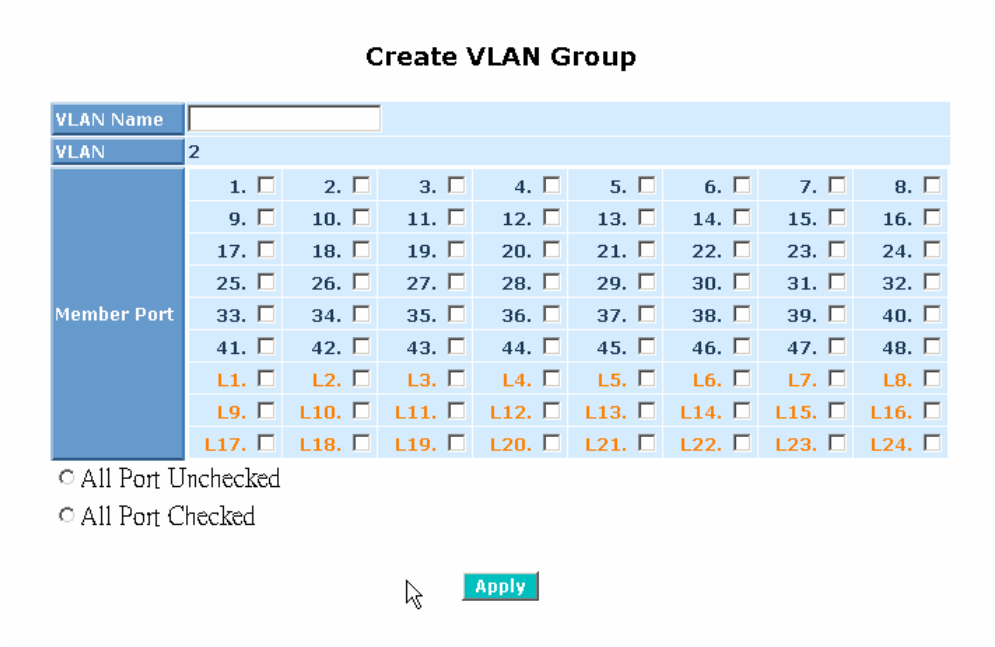



Fig. 3-60

### 3-21-3. Port Protocol

*Function name:*

Port Protocol Setting

*Function description:*

Protocol-based VLAN is based on 802.1q tag VLAN and is a kind of classification rules based on PVID configuration. You must apply tagged VLAN first. In switch, it supports IPv4, IPv6, ARP, RARP, User Defined 0, User Defined 1, User Defined 2,and Other. When the packets having no vlan's tag enter the port 1 of the switch and belong to ipv4 and, the switch will add PVID to the packets. It will follow the rule of the configuration of VLAN Port Protocol Setting. If the packets have specific tag and VID, it will follow the rule of the configuration of VLAN tagged group straight.

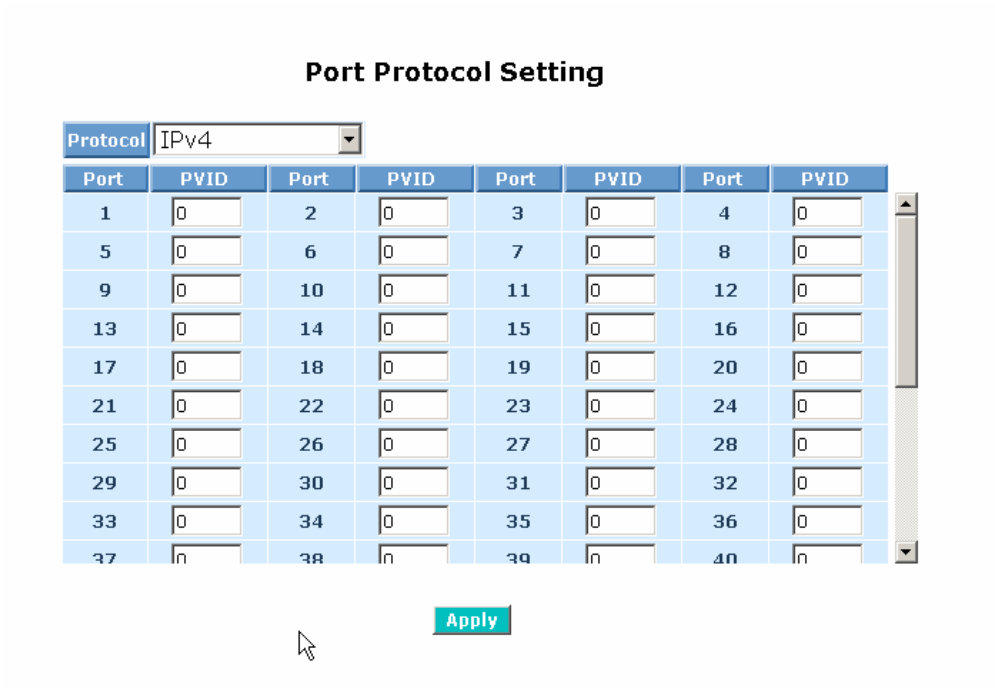



Fig. 3-61

*Parameter description:*

Protocol:

Including IPv4, IPv6, ARP, RARP, User Defined 0, User Defined 1, User Defined 2, and Other. User 0~2 would be determined in User Defined function.

Port 1~48:

Port number.

PVID:

In PVID Setting, you can assign Port Permanent VLAN ID to each port for untagged packets that enter the switch and operate in designated VLAN group after adding the VLAN tag according to PVID. The range of PVID number is the same as VID from 1 to 4094. Usually, before you set a number x as PVID, you would create a Tag-based VLAN with VID x. Because if port 1 receives an untagged packet, the switch will add PVID (assume VID 2) to this packet and make it have tag, the packet will be forward to VLAN group of VID 2 you have created in advance in the switch.

### 3-21-4. Port VID

*Function name:*

Port VID

*Function description:*

Port VID is applied to untagged packets entering the switch. The packets will add VID and forward in this VID group according to PVID number. In the switch, VLAN has different Modes to run in all kinds of network environment. The switch supports four modes being Access, Private, Trunk, and Hybrid. When apply “Access” mode, the switch only accept untagged packets; otherwise, it will discard these packets. The ports applying “Access” mode also can’t transmit untagged packets. The behavior of “Private” Mode is the same as “Access” Mode basically. The only one different point is that Private ports couldn’t communicate with Private ports or Access Ports but could communicate with Trunk ports or Hybrid ports. In “Trunk” mode, the trunk ports only accept tagged packets; otherwise, they will discard the packets. Trunk ports would only transmit tagged packets. In “Hybrid” mode, the trunk ports only accept tagged packets as well; otherwise, they will discard the packets. Trunk ports would only transmit tagged packets but have a exception being that when VID of VLAN group of the packets is the same as PVID of the port, the packets transmitting out of the switch will have no tag.

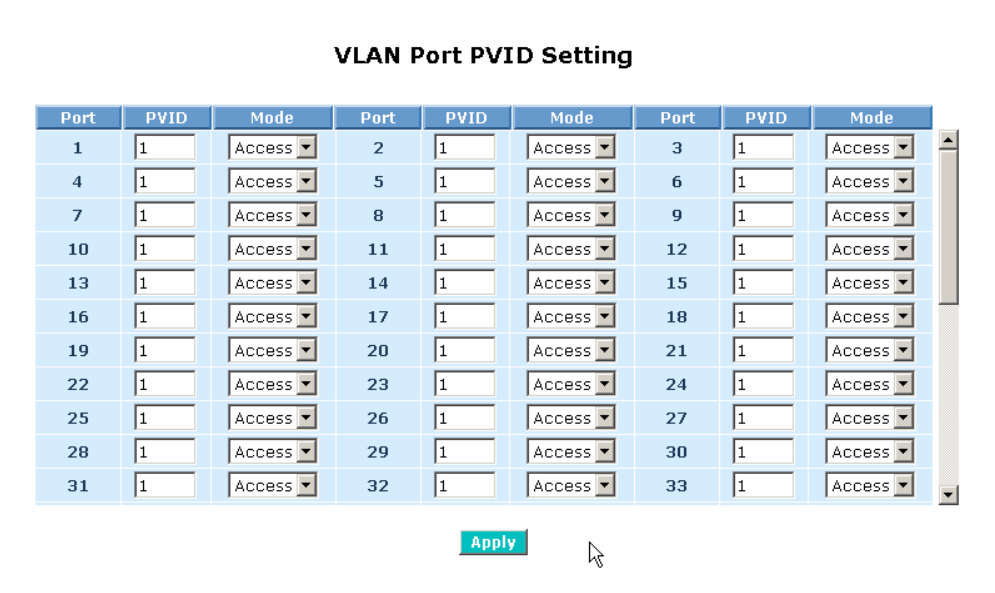

VLAN Port PVID Setting
Port PVID Mode Port PVID Mode Port PVID Mode
1 1 Access 2 1 Access 3 1 Access
4 1 Access 5 1 Access 6 1 Access
7 1 Access 8 1 Access 9 1 Access
10 1 Access 11 1 Access 12 1 Access
13 1 Access 14 1 Access 15 1 Access
16 1 Access 17 1 Access 18 1 Access
19 1 Access 20 1 Access 21 1 Access
22 1 Access 23 1 Access 24 1 Access
25 1 Access 26 1 Access 27 1 Access
28 1 Access 29 1 Access 30 1 Access
31 1 Access 32 1 Access 33 1 Access
Apply

Fig. 3-62

*Parameter description:*

Port 1-48:

Port number.

PVID:

This PVID range could be 1-4094. Before you set a number x as PVID, you have to create a Tag-based VLAN with VID x. For example, if port x receives an untagged packet, the switch will apply the PVID (assume as VID y) of port x and add tag to this packet, the packet then will be forwarded as the tagged packet with VID y.

Mode:

Here you can choose Access, Trunk or Hybrid. After your selecting, press the **<Apply>** button to have the setting taken effect.

## 3-22. Reboot

We offer you many ways to reboot the switch, including to close and open power supply, hardware reset and software reset. You can press the RESET button in the front panel to reset the switch. Here that we are discussing is software reset .

*Function name:*

Reboot

*Function description:*

Reboot the switch. Reboot takes the same effect as the RESET button on the front panel of the switch. It will take around thirty (30) seconds to complete the system boot.

*Parameter description:*

Save and Reboot:

Save the current settings as start configuration before rebooting the switch and then reboot the system.

Reboot:

Reboot the system directly.

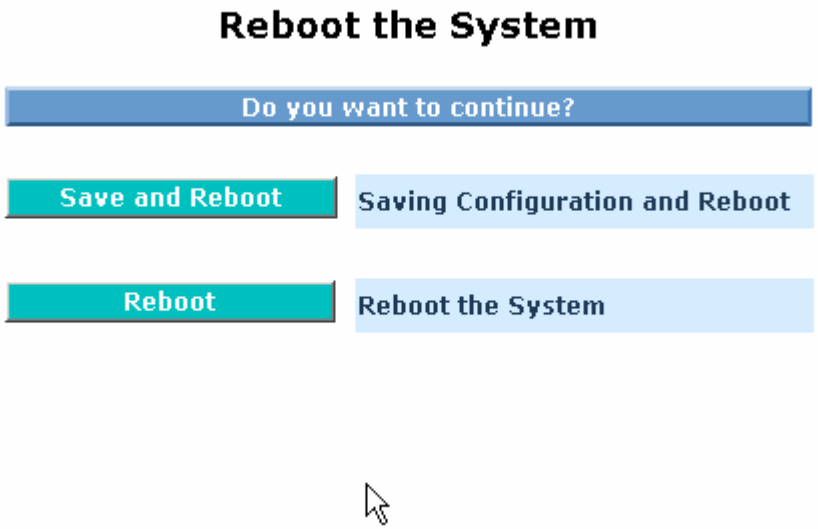



Fig. 3-63

## 3-23. Logout

You can manually logout in Logout function. In the switch, you could decide the time for auto-logout in Auto Logout capability above the Web UI. It could prevent the network administrator from forgetting logout Web UI operating interface. Turn "Auto Logout" as OFF and the users will not be logout forever.

*Function name:*

Logout

*Function description:*

The switch allows you to logout the system to prevent other users from entering the system without the permission. Besides this manually logout, You can use implicit logout by clicking **<Auto Logout>** radian at the right-top corner to explicitly ON/OFF this logout function.

*Parameter description:*

Logout:

Press the **<Logout>** button to have you logout straightly.

Auto Logout:

Select On/OFF. Default is ON. If it is "3 min", and no action and no key is stroke as well. After 3 minutes, the switch will have you logout automatically.

Fig. 3-64

# 4. Operation of CLI Management

## *4-1. CLI Management*

Refer to Chapter 2 for basic installation. The following description is the brief of the network connection.

-- Locate the correct DB-9 null modem cable with female DB-9 connector. Null modem cable comes with the management switch. Refer to the Appendix B for null modem cable configuration.

-- Attach the DB-9 female connector to the male DB-9 serial port connector on the Management board.

-- Attach the other end of the DB-9 cable to an ASCII terminal emulator or PC Com-1, 2 port. For example, PC runs Microsoft Windows HyperTerminal utility.

-- At “Com Port Properties” Menu, configure the parameters as below: (see the next section)

| | |
|---|---|
| Baud rate | 57600 |
| Stop bits | 1 |
| Data bits | 8 |
| Parity | N |
| Flow control | none |

### *4-1-1. Login*

The command-line interface (CLI) is a text-based interface. User can access the CLI through either a direct serial connection to the device or a Telnet session. The default values of the managed switch are listed below:

Username: admin
Password: admin

After you login successfully, the prompt will be shown as “**#**“ if you are the first login person and your authorization is administrator; otherwise it may show “**$**“. See the following two figures. The former means you behave as an administrator and have the access right of the system. As to the latter, it means you behave as a guest and are only allowed to view the system without the permission to do any setting for this switch.

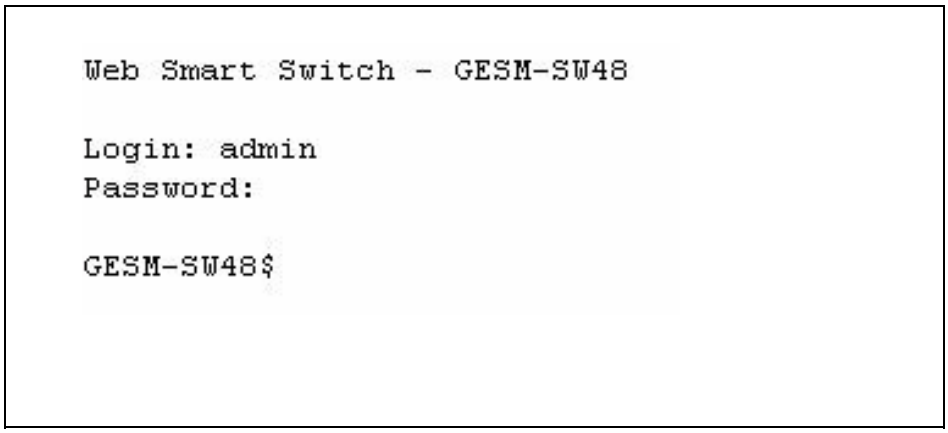

Web Smart Switch - GESM-SW48
Login: admin
Password:
GESM-SW48$

Fig. 4-1

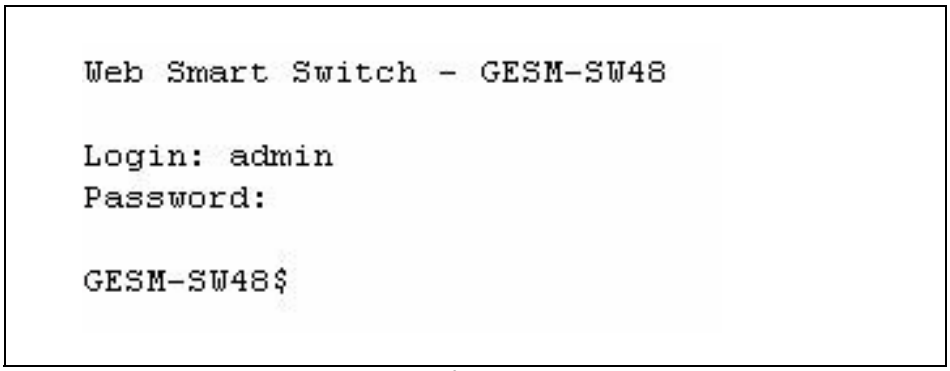

Web Smart Switch - GESM-SW48
Login: admin
Password:
GESM-SW48$

Fig. 4-2

## 4-2. Commands of CLI

To see the commands of the mode, please input "**?**" after the prompt, then all commands will be listed in the screen. All commands can be divided into two categories, including global commands and local commands. Global commands can be used wherever the mode you are. They are "exit", "end", "help", "history", "logout", "save start", "save user", "restore default" and "restore user". For more details, please refer to Section 4-2-1.

Command instructions reside in the corresponding modes are local commands. The same command with the same command name may occur but perform totally different function in different modes. For example, "show" in IP mode performs displaying the IP information; however, it performs displaying the system information in system mode. For more details, please refer to Section 4-2-2.

```
Web Smart Switch - GESM-SW48

Login: admin
Password:

GESM-SW48# ?
  autologout            Change autologout time
  hostname              Change hostname
  ip                    Enter into ip mode
  reboot                Reboot the system
  system                Enter into system mode
  ------------<< Global commands >>------------
  end                   Back to the top mode
  exit                  Back to the previous mode
  help                  Show available commands
  history               Show a list of previously run commands
  logout                Logout the system
  restore               Restore default or user config
  save                  Save as start or user config

GESM-SW48#
```

Fig. 4-3

### 4-2-1. Global Commands of CLI

*end*

**Syntax:**
end
**Description:**
Back to the top mode.
When you enter this command, your current position would move to the top mode. If you use this command in the top mode, you are still in the position of the top mode.
**Argument:**
None.
**Possible value:**
None.
**Example:**

```
LGB2048A# ip
LGB2048A(ip)# end

LGB2048A#
```

*exit*

**Syntax**:
exit
**Description**:
Back to the previous mode.
When you enter this command, your current position would move back to the previous mode. If you use this command in the top mode, you are still in the position of the top mode.
**Argument**:
None.
**Possible value:**
None.
**Example:**

```
LGB2048A# ip
LGB2048A(ip)# exit

LGB2048A#
```

*help*

**Syntax:**
help
**Description:**
To show available commands.
Some commands are the combination of more than two words. When you enter this command, the CLI would show the complete commands. Besides, the command would help you classify the commands between the local commands and the global ones.
**Argument:**
None.
**Possible value:**
None.
**Example:**

```
LGB2048A# ip
LGB2048A(ip)# help
Commands available:
  ------------<< Local commands >>------------
  set dns              Set dns
  set ip               Set ip,subnet mask and gateway
  show                 Show IP Configuration
  ------------<< Global commands >>------------
  end                  Back to the top mode
  exit                 Back to the previous mode
  help                 Show available commands
  history              Show a list of previously run commands
  logout               Logout the system
  restore default      Restore default config
  restore user         Restore user config
  save start           Save as start config
  save user            Save as user config
```

*history*

**Syntax:**
history [#]
**Description:**
To show a list of previous commands that you had ever run.
When you enter this command, the CLI would show a list of commands which you had typed before. The CLI supports up to 256 records. If no argument is typed, the CLI would list total records up to 256. If optional argument is given, the CLI would only show the last numbers of records, given by the argument.
**Argument:**
[#]: show last number of history records. (optional)
**Possible value:**
[#]: 1, 2, 3, …., 256
**Example:**

```
LGB2048A(ip)# history
 Command history:
   0. trunk
   1. exit
   2. LGB2048A# trunk
   3. LGB2048A(trunk)# exit
   4. LGB2048A#
   5. ?
   6. trunk
   7. exit
   8. alarm
   9. events
  10. end
  11. ip
  12. help
  13. ip
  14. history

LGB2048A(ip)# history 3
 Command history:
  13. ip
  14. history
  15. history 3

LGB2048A(ip)#
```

*logout*

**Syntax:**
logout
**Description:**
When you enter this command via Telnet connection, you would logout the system and disconnect. If you connect the system through direct serial port with RS-232 cable, you would logout the system and be back to the initial login prompt when you run this command.
**Argument:**
None.
**Possible value:**
None.
**Example:**
LGB2048A# logout

*restore default*

**Syntax:**
restore default
**Description:**
When you use this function in CLI, the system will show you the information “Do you want to restore the default IP address?(y/n)”. If you choose Y or y, the IP address will restore to default “192.168.1.1”. If you choose N or n, the IP address will keep the same one that you had saved before.

If restoring default successfully, the CLI would prompt if reboot immediately or not. If you press Y or y, the system would reboot immediately; otherwise, it would be back to the CLI system. After restoring default configuration, all the changes in the startup configuration would be lost. After rebooting, the entire startup configuration would reset to factory default.

**Argument:**
None.
**Possible value:**
None.
**Example:**
LGB2048A# restore default
Do you want to restore the default ip address?(y/n)
Restoring ...
Restore Default Configuration Successfully
Do you want to reboot the system?(y/n)

*Restore user*

**Syntax:**
restore user
**Description:**
To restore the startup configuration as user defined configuration. If restoring default successfully, the CLI would prompt if reboot immediately or not. If you press Y or y, the system would reboot immediately; others would back to the CLI system. After restoring user-defined configuration, all the changes in the startup configuration would be lost. After rebooting, the entire startup configuration would replace as user defined one.
**Argument:**
None.
**Possible value:**
None.
**Example:**
LGB2048A# restore user
Restoring ...
Restore User Configuration Successfully
Press any key to reboot system.

*save start*

**Syntax:**
save start
**Description:**
To save the current configuration as the start one. When you enter this command, the CLI would save your current configuration into the non-volatile FLASH. If you want the configuration still works after rebooting, save the configuration using the command ‘save start’.
**Argument:**
None.
**Possible value:**
None.
**Example:**
LGB2048A# save start
Saving start...
Save Successfully

LGB2048A#

*save user*

**Syntax:**
save user
**Description:**
To save the current configuration as the user-defined configuration. When you enter this command, the CLI would save your current configuration into the non-volatile FLASH as user-defined configuration.
**Argument:**
None.
**Possible value:**
None.
**Example:**
LGB2048A# save user
Saving user...
Save Successfully

LGB2048A#

### 4-2-2. Local Commands of CLI

#### ■ autologout

*autologout*

**Syntax**:
autologout <time>
**Description**:
To set up the timer of autologout.
**Argument**:
<time>: range 1 to 3600 seconds, 0 for autologout off, current setting is 180 seconds.
**Possible value:**
<time>: 0,1-3600
**Example:**
LGB2048A# autologout 3600
Set autologout time to 3600 seconds

#### ■ hostname

*hostname*

**Syntax**:
hostname <name>
**Description**:
To set up the hostname of the switch.
**Argument**:
<name>: hostname, max. 40 characters.
**Possible value:**
<name>: hostname, max. 40 characters.
**Example:**
LGB2048A# hostname Company

Company#

■ **IP**

*set dns*

**Syntax**:
set dns <ip>
**Description**:
To set the IP address of DNS server.
**Argument**:
<ip> : dns ip address
**Possible value:**
168.95.1.1
**Example:**
LGB2048A (ip)# set dns 168.95.1.1

*set ip*

**Syntax**:
set ip <ip> <mask> <gateway>
**Description**:
To set the system IP address, subnet mask and gateway.
**Argument**:
<ip> : ip address
<mask> : subnet mask
<gateway> : default gateway
**Possible value:**
<ip> : 192.168.1.2 or others
<mask> : 255.255.255.0 or others
<gateway> : 192.168.1.253 or others
**Example:**
LGB2048A(ip)# set ip 192.168.1.2 255.255.255.0 192.168.1.253

*show*

**Syntax**:
show
**Description**:
To display the system's IP address, subnet mask, default gateway, DNS mode, and DNS server IP address.
**Argument**:
None
**Possible value:**
None
**Example:**
LGB2048A(ip)# show

```
IP Address          : 192.168.1.1
Subnet mask         : 255.255.255.0
Gateway             : 192.168.1.254
DNS Setting         : Manual
DNS Server          : 168.95.1.1
```

### ■ reboot

*reboot*

**Syntax:**
reboot
**Description:**
To reboot the system.
**Argument:**
None.
**Possible value:**
None.
**Example:**
LGB2048A# reboot

## ■ system

*set contact*

**Syntax**:
set contact <contact string>
**Description**:
To set the contact description of the switch.
**Argument**:
<contact>:string length up to 40 characters.
**Possible value:**
<contact>: A, b, c, d, ... ,z and 1, 2, 3, …. etc.
**Example:**
LGB2048A(system)# set contact Taipei

*set device-name*

**Syntax**:
set device-name <device-name string>
**Description**:
To set the device name description of the switch.
**Argument**:
<device-name>: string length up to 40 characters.
**Possible value:**
<device-name>: A, b, c, d, ... ,z and 1, 2, 3, …. etc.
**Example:**
LGB2048A(system)# set device-name GS-1148

*set location*

**Syntax**:
set location <location string>
**Description**:
To set the location description of the switch.
**Argument**:
<location>: string length up to 40 characters.
**Possible value:**
<location>: A, b, c, d, ... ,z and 1, 2, 3, …. etc.
**Example:**
LGB2048A(system)# set location Taipei

*show*

**Syntax**:
show
**Description**:
To display the basic information of the switch.
**Argument**:
None.
**Possible value:**
None.
**Example:**

```
LGB2048A(system)# show
Model Name                    : LGB2048A
System Description            : 48-Port 10/100/1000M Gigabit SW.
Location                      :
Contact                       :
Device Name                   : LGB2048A
System Up Time                : 0 Days 0 Hours 4 Mins 14 Secs
Current Time                  : Tue Jan 17 16:28:46 2006
BIOS Version                  : v1.00
Firmware Version              : v1.05
Hardware-Mechanical Version   : v1.01-v1.01
Serial Number                 : 031A02000001
Host IP Address               : 192.168.1.1
Host MAC Address              : 00-40-c7-3b-00-cb
Device Port                   : UART * 1, TP * 44, Dual-Media Port(RJ45/SFP)
* 4
RAM Size                      : 64 M
Flash Size                    : 16 M
```

# 5. FAQ

## 5-1. Resolving No Link Condition

The possible causes for a no link LED status are as follows:

- The attached device is not powered on
- The cable may not be the correct type or is faulty
- The installed building premise cable is faulty
- The port may be faulty

## 5-2. Q&A

1. Computer A can connect to Computer B, but cannot connect to Computer C through the Gigabit Web Smart Switch.
   - ✓ The network device of Computer C may fail to work. Please check the link/act status of Computer C on the LED indicator. Try another network device on this connection.
   - ✓ The network configuration of Computer C may be something wrong. Please verify the network configuration on Computer C.

2. The uplink connection function fails to work.
   - ✓ The connection ports on another must be connection ports. Please check if connection ports are used on that Gigabit Web Smart Switch.
   - ✓ Please check the uplink setup of the Gigabit Web Smart Switch to verify the uplink function is enabled.

3. The console interface cannot appear on the console port connection.
   - ✓ Gigabit Web Smart Switch has no console port, so you cannot use console interface to connect with Gigabit Web Smart Switch.

4. How to configure the Gigabit Web Smart Switch.
   - ✓ User can use Web browser program in window series of computer to control the web smart functions in Gigabit Web Smart Switch. First, choose any port in Gigabit Web Smart Switch. Then, use browser and type default IP address, 192.168.1.1, to connect to Gigabit with RJ45 network line. Finally, the login screen will appear at once.

# Appendix A
# Technical Specifications

### *Features*

- 44 (10/100/1000Mbps) Gigabit Ethernet (TP) switching ports are compliant with IEEE802.3, 802.3u, 802.3z and 802.3ab.
- 4 Gigabit TP/SFP fiber are dual media ports with auto detected function.
- Non-blocking store-and-forward shared-memory Web-Smart switched.
- Supports auto-negotiation for configuring speed, duplex mode.
- Supports 802.3x flow control for full-duplex ports.
- Supports collision-based and carrier-based backpressure for half-duplex ports.
- Any ports can be in disable mode, force mode or auto-polling mode.
- Supports Head of Line (HOL) blocking prevention.
- Supports broadcast storm filtering.
- Web-based management provides the ability to completely manage the switch.
- Supports Port-based VLAN and Tag-based VLAN.
- Auto-aging with programmable inter-age time.
- Supports 802.1p Class of Service with 8 level priority queuing.
- Supports port trunking with flexible load distribution and failover function.
- Supports port sniffer function
- Programmable maximum Ethernet frame length of 16KB jumbo frame.
- Efficient self-learning and address recognition mechanism enables forwarding rate at wire speed.

### *Hardware Specifications*

- **Standard Compliance:** IEEE802.3/802.3ab / 802.3z / 802.3u / 802.3x
- **Network Interface:**

| Configuration | Mode | Connector | Port |
|---|---|---|---|
| 10/100/1000Mbps Gigabit TP | NWay | TP (RJ-45) | 1 – 48 |
| 1000Base-SX Gigabit Fiber | 1000 FDX | *SFP | 44-48 (Option) |
| 1000Base-LX Gigabit Fiber | 1000 FDX | *SFP | 44-48 (Option) |
| 1000Base-LX Single Fiber WDM (BiDi) | 1000 FDX | *SFP | 44-48 (Option) |

*Port 44-48 are TP/SFP fiber dual media ports with auto detected function
*Optional SFP module supports LC or BiDi LC transceiver

- **Transmission Mode:** 10/100Mbps support full or half duplex
  1000Mbps support full duplex only
- **Transmission Speed:** 10/100/1000Mbps for TP
  1000Mbps for Fiber
- **Full Forwarding/Filtering Packet Rate:** PPS (packets per second)

| Forwarding Rate | Speed |
|---|---|
| 1,488,000PPS | 1000Mbps |
| 148,800PPS | 100Mbps |
| 14,880PPS | 10Mbps |

- **MAC Address and Self-learning:** 8K MAC address
  256 VLAN table entries,
- **Flow Control:** IEEE802.3x compliant for full duplex
  Backpressure flow control for half duplex
- **Cable and Maximum Length:**

| | |
|---|---|
| **TP** | Cat. 5 UTP cable, up to 100m |
| **1000Base-SX** | Up to 220/275/500/550m, which depends on Multi-Mode Fiber type |
| **1000Base-LX** | Single-Mode Fiber, up to10/30/50Km |
| **1000Base-LX WDM (BiDi)** | Single-Mode Single Fiber, up to 20Km |

- **Diagnostic LED:**

  System LED : Power, CPU
  Per Port LED:
  10/100/1000M TP Port 1 to 44 : LINK/ACT, 10/100/1000Mbps
  1000M SFP Fiber Port 44-48 : SFP(LINK/ACT)

- **Power Requirement** **:** AC Line

  Voltage : 100~240 V
  Frequency : 50~60 Hz
  Consumption : 85W
- **Ambient Temperature** **:** 0° to 40°C
- **Humidity** **:** 5% to 90%
- **Dimensions** **:** 44(H) × 442(W) × 248.6(D) mm
- **Comply with FCC Part 15 Class A & CE Mark Approval**

*Publication date: Feb., 2008*
*Revision A1*